Scan Report

June 27, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “window CW”. The scan started at Thu Jun 27 10:06:22 2024 UTC and ended at Thu Jun 27 10:57:34 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.56.103	379	213	36	0	0
Total: 1	379	213	36	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 628 results selected by the filtering described above. Before filtering there were 841 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.56.103	SMB	Success	Protocol SMB, Port 445, User vagrant

2 Results per Host

2.1 192.168.56.103

Host scan start Thu Jun 27 10:06:58 2024 UTC
Host scan end Thu Jun 27 10:57:26 2024 UTC

Service (Port)	Threat Level
general/tcp	High
9200/tcp	High
21/tcp	High
3389/tcp	High
3306/tcp	High
8383/tcp	High
1617/tcp	High
80/tcp	High
22/tcp	High

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
8009/tcp	High
8282/tcp	High
445/tcp	High
135/tcp	Medium
general/tcp	Medium
9200/tcp	Medium
21/tcp	Medium
3389/tcp	Medium
3306/tcp	Medium
3820/tcp	Medium
8383/tcp	Medium
4848/tcp	Medium
3920/tcp	Medium
22/tcp	Medium
8181/tcp	Medium
8282/tcp	Medium
general/icmp	Low
general/tcp	Low
9200/tcp	Low
3306/tcp	Low
22/tcp	Low

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Microsoft Windows NAT Driver Denial of Service Vulnerability (2849568)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-062.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to execute arbitrary code and take complete control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2012
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

Flaw is due to an improper handling asynchronous RPC requests.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows NAT Driver Denial of Service Vulnerability (2849568)`

OID:1.3.6.1.4.1.25623.1.0.903317

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-3175
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-062
url: http://www.securityfocus.com/bid/61673
url: http://support.microsoft.com/default.aspx?scid=kb;EN-US;2849470
dfn-cert: DFN-CERT-2013-1471
```

High (CVSS: 10.0)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (2969262)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS14-035.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to conduct session hijacking attacks, disclose potentially sensitive information, bypass certain security restrictions, and compromise a user's system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws are due to:
- A use-after-free error when handling CMarkup objects.
- An error when handling negotiation of certificates during a TLS session.
- Improper validation of certain permissions.
- and multiple Unspecified errors.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (2969262)`
OID:1.3.6.1.4.1.25623.1.0.804595
Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-0282
cve: CVE-2014-1762
cve: CVE-2014-1764
cve: CVE-2014-1766
cve: CVE-2014-1769
cve: CVE-2014-1770
cve: CVE-2014-1771
cve: CVE-2014-1772
cve: CVE-2014-1773
cve: CVE-2014-1774
cve: CVE-2014-1775
cve: CVE-2014-1777
cve: CVE-2014-1778
cve: CVE-2014-1779
cve: CVE-2014-1780
cve: CVE-2014-1781
cve: CVE-2014-1782
cve: CVE-2014-1783
cve: CVE-2014-1784
cve: CVE-2014-1785
cve: CVE-2014-1786
cve: CVE-2014-1788
cve: CVE-2014-1789
cve: CVE-2014-1790
cve: CVE-2014-1791
cve: CVE-2014-1792
cve: CVE-2014-1794
cve: CVE-2014-1795
cve: CVE-2014-1796
cve: CVE-2014-1797
cve: CVE-2014-1799
cve: CVE-2014-1800
cve: CVE-2014-1802
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-1803
cve: CVE-2014-1804
cve: CVE-2014-1805
cve: CVE-2014-2753
cve: CVE-2014-2754
cve: CVE-2014-2755
cve: CVE-2014-2756
cve: CVE-2014-2757
cve: CVE-2014-2758
cve: CVE-2014-2759
cve: CVE-2014-2760
cve: CVE-2014-2761
cve: CVE-2014-2763
cve: CVE-2014-2764
cve: CVE-2014-2765
cve: CVE-2014-2766
cve: CVE-2014-2767
cve: CVE-2014-2768
cve: CVE-2014-2769
cve: CVE-2014-2770
cve: CVE-2014-2771
cve: CVE-2014-2772
cve: CVE-2014-2773
cve: CVE-2014-2775
cve: CVE-2014-2776
cve: CVE-2014-2777
url: https://support.microsoft.com/kb/2957689
url: http://www.securityfocus.com/bid/67295
url: http://www.securityfocus.com/bid/67511
url: http://www.securityfocus.com/bid/67518
url: http://www.securityfocus.com/bid/67544
url: http://www.securityfocus.com/bid/67831
url: http://www.securityfocus.com/bid/67833
url: http://www.securityfocus.com/bid/67834
url: http://www.securityfocus.com/bid/67835
url: http://www.securityfocus.com/bid/67836
url: http://www.securityfocus.com/bid/67838
url: http://www.securityfocus.com/bid/67839
url: http://www.securityfocus.com/bid/67840
url: http://www.securityfocus.com/bid/67841
url: http://www.securityfocus.com/bid/67842
url: http://www.securityfocus.com/bid/67843
url: http://www.securityfocus.com/bid/67845
url: http://www.securityfocus.com/bid/67846
url: http://www.securityfocus.com/bid/67847
url: http://www.securityfocus.com/bid/67848
url: http://www.securityfocus.com/bid/67849
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/67850
url: http://www.securityfocus.com/bid/67851
url: http://www.securityfocus.com/bid/67852
url: http://www.securityfocus.com/bid/67854
url: http://www.securityfocus.com/bid/67855
url: http://www.securityfocus.com/bid/67856
url: http://www.securityfocus.com/bid/67857
url: http://www.securityfocus.com/bid/67858
url: http://www.securityfocus.com/bid/67859
url: http://www.securityfocus.com/bid/67860
url: http://www.securityfocus.com/bid/67861
url: http://www.securityfocus.com/bid/67862
url: http://www.securityfocus.com/bid/67863
url: http://www.securityfocus.com/bid/67864
url: http://www.securityfocus.com/bid/67866
url: http://www.securityfocus.com/bid/67867
url: http://www.securityfocus.com/bid/67869
url: http://www.securityfocus.com/bid/67871
url: http://www.securityfocus.com/bid/67872
url: http://www.securityfocus.com/bid/67873
url: http://www.securityfocus.com/bid/67874
url: http://www.securityfocus.com/bid/67875
url: http://www.securityfocus.com/bid/67876
url: http://www.securityfocus.com/bid/67877
url: http://www.securityfocus.com/bid/67878
url: http://www.securityfocus.com/bid/67879
url: http://www.securityfocus.com/bid/67880
url: http://www.securityfocus.com/bid/67881
url: http://www.securityfocus.com/bid/67882
url: http://www.securityfocus.com/bid/67883
url: http://www.securityfocus.com/bid/67884
url: http://www.securityfocus.com/bid/67885
url: http://www.securityfocus.com/bid/67886
url: http://www.securityfocus.com/bid/67887
url: http://www.securityfocus.com/bid/67889
url: http://www.securityfocus.com/bid/67890
url: http://www.securityfocus.com/bid/67891
url: http://www.securityfocus.com/bid/67892
url: http://www.securityfocus.com/bid/67915
url: https://support.microsoft.com/kb/2963950
url: https://technet.microsoft.com/library/security/ms14-035
cert-bund: CB-K14/0713
cert-bund: CB-K14/0628
```

High (CVSS: 10.0)
NVT: Microsoft Internet Explorer Remote Code Execution Vulnerability (2965111)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-021.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
The flaw exists in the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Remote Code Execution Vulnerability (2965111)`
OID:1.3.6.1.4.1.25623.1.0.804441
Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-1776
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://secpod.org/blog/?p=2512
url: http://www.securityfocus.com/bid/67075
url: http://www.kb.cert.org/vuls/id/222929
url: https://technet.microsoft.com/library/security/2963983
url: http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targ
↪eting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.h
↪tml
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-021
cert-bund: CB-K14/0487
```

High (CVSS: 10.0)
NVT: Microsoft .NET Framework Privilege Elevation Vulnerability (2958732)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-026.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow an attacker to bypass certain security restrictions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 1.1, 2.0, 3.5, 3.5.1, 4.0 and 4.5 and 4.5.1.

Vulnerability Insight
The flaw is due to the framework not properly restricting access to certain application objects related to TypeFilterLevel checks.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Privilege Elevation Vulnerability (2958732)`
OID:1.3.6.1.4.1.25623.1.0.804452
Version used: `2023-07-27T05:05:08Z`

References

```
cve: CVE-2014-1806
url: http://support.microsoft.com/kb/2958732
url: http://www.securityfocus.com/bid/67286
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms
↪14-026
cert-bund: CB-K14/0568
```

High (CVSS: 10.0)
NVT: Microsoft Windows Print Spooler Remote Code Execution Vulnerability (2769369)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS13-001.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation could allow remote attackers to execute arbitrary code by sending a specially crafted print job to the print server.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

The vulnerability is caused when the Windows Print Spooler fails to handle a specially crafted print job.

Vulnerability Detection Method

Details: `Microsoft Windows Print Spooler Remote Code Execution Vulnerability (2769369)`

OID:1.3.6.1.4.1.25623.1.0.901213

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-0011
url: http://support.microsoft.com/kb/2769369
url: http://www.securityfocus.com/bid/57142
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-001
dfn-cert: DFN-CERT-2013-0043
```

High (CVSS: 10.0)

NVT: Microsoft .NET Framework Privilege Elevation Vulnerability (2800277)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-015.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow an attacker to execute arbitrary code.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 2.0 Service Pack 2

Vulnerability Insight

The flaw is due to an error when handling permissions of a callback function when a certain WinForm object is created and can be exploited to bypass CAS (Code Access Security) restrictions via a specially crafted XAML Browser Application (XBAP) or an untrusted .NET application.

Vulnerability Detection Method

Details: `Microsoft .NET Framework Privilege Elevation Vulnerability (2800277)`
OID:1.3.6.1.4.1.25623.1.0.902950
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-0073
url: http://support.microsoft.com/kb/2800277
url: http://www.securityfocus.com/bid/57847
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-015
dfn-cert: DFN-CERT-2013-0292
```

High (CVSS: 10.0)
NVT: Microsoft Internet Explorer (IE) End of Life (EOL) Detection

Summary

The Microsoft Internet Explorer (IE) version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result

```
The "Microsoft Internet Explorer (IE)" version on the remote host has reached th
↪e end of life.
CPE:               cpe:/a:microsoft:ie:8.0.7601.17514
Installed version: 8.0.7601.17514
Location/URL:      C:\Program Files (x86)\Internet Explorer
EOL version:       < 11.x
EOL date:          N/A
```

Impact

An EOL version of Microsoft IE is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update the Microsoft IE version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: `Microsoft Internet Explorer (IE) End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.806657
Version used: `2022-06-21T10:45:58Z`

References
`url: https://support.microsoft.com/en-us/lifecycle#gp/Microsoft-Internet-Explore`
`↪r`

High (CVSS: 10.0)
NVT: Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2761226)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-075.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow remote attackers to execute arbitrary code with kernel-mode privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to
- Use-after-free error within win32k.sys when handling objects in memory.
- An error when parsing a specially crafted 'TrueType' font file.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (27.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.902693

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-2530
cve: CVE-2012-2553
cve: CVE-2012-2897
url: http://support.microsoft.com/kb/2761226
url: http://www.securityfocus.com/bid/56447
url: http://www.securityfocus.com/bid/56448
url: http://www.securityfocus.com/bid/56457
url: https://technet.microsoft.com/en-us/security/bulletin/ms12-075
dfn-cert: DFN-CERT-2012-2110
```

High (CVSS: 10.0)

NVT: Microsoft .NET Framework Remote Code Execution Vulnerability (3000414)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS14-057.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to bypass certain security restrictions and compromise a vulnerable system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.0, 4.5, 4.5.1 and 4.5.2.

Vulnerability Insight

Multiple flaws are due to:

- An unspecified error related to .NET ClickOnce.
- An unspecified error when handling internationalized resource identifiers.
- An unspecified error.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Microsoft .NET Framework Remote Code Execution Vulnerability (3000414)`
OID:1.3.6.1.4.1.25623.1.0.804777
Version used: `2023-07-27T05:05:08Z`

References

```
cve: CVE-2014-4073
cve: CVE-2014-4121
cve: CVE-2014-4122
url: https://support.microsoft.com/kb/3000414
url: http://www.securityfocus.com/bid/70312
url: http://www.securityfocus.com/bid/70313
url: http://www.securityfocus.com/bid/70351
url: https://technet.microsoft.com/library/security/ms14-057
cert-bund: CB-K14/1292
```

High (CVSS: 10.0)
NVT: Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (3042553)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-034.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight

Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (3042553)
OID:1.3.6.1.4.1.25623.1.0.805370
Version used: 2023-07-25T05:05:58Z

References

```
cve: CVE-2015-1635
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/3042553
url: https://technet.microsoft.com/library/security/MS15-034
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545
```

High (CVSS: 10.0)
NVT: Apache Log4j End of Life (EOL) Detection - Windows

Summary

The Apache Log4j version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result

```
The "Apache Log4j" version on the remote host has reached the end of life.
CPE:               cpe:/a:apache:log4j:1.2.17
Installed version: 1.2.17
Location/URL:      C:\Program Files\Apache Software Foundation\tomcat\apache-tom
↪cat-8.0.33\webapps\struts2-rest-showcase\WEB-INF\lib\log4j-1.2.17.jar
EOL version:       1.2
EOL date:          2015-08-05
EOL info:          https://blogs.apache.org/foundation/entry/apache_logging_serv
↪ices_project_announces
```

Impact

An EOL version of Apache Log4j is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

Solution type: VendorFix
Update the Apache Log4j version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if an EOL version is present on the target host.
Details: Apache Log4j End of Life (EOL) Detection - Windows
OID:1.3.6.1.4.1.25623.1.0.117844
Version used: 2021-12-17T14:24:48Z

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://blogs.apache.org/foundation/entry/apache_logging_services_project_a
↪nnounces
```

High (CVSS: 10.0)
NVT: Apache Log4j End of Life (EOL) Detection - Windows

Summary

The Apache Log4j version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result

```
The "Apache Log4j" version on the remote host has reached the end of life.
CPE:               cpe:/a:apache:log4j:1.2.15
Installed version: 1.2.15
Location/URL:      C:\Program Files\Apache Software Foundation\tomcat\apache-tom
↪cat-8.0.33\webapps\axis2\WEB-INF\lib\log4j-1.2.15.jar
EOL version:       1.2
EOL date:          2015-08-05
EOL info:          https://blogs.apache.org/foundation/entry/apache_logging_serv
↪ices_project_announces
```

Impact

An EOL version of Apache Log4j is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix
Update the Apache Log4j version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if an EOL version is present on the target host.
Details: `Apache Log4j End of Life (EOL) Detection - Windows`
OID:1.3.6.1.4.1.25623.1.0.117844
Version used: `2021-12-17T14:24:48Z`

References

```
url: https://blogs.apache.org/foundation/entry/apache_logging_services_project_a
↪nnounces
```

High (CVSS: 10.0)
NVT: Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2783534)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-078.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code with kernel-mode privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
- An error in the OpenType Font (OTF) driver when handling certain objects can be exploited via a specially crafted font file.
- An error when handling certain TrueType Fonts (TTF) can be exploited via a specially crafted font file.

Vulnerability Detection Method
Details: `Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (27.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902936
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-2556
cve: CVE-2012-4786
url: http://support.microsoft.com/kb/2753842
url: http://www.securityfocus.com/bid/56841
url: http://www.securityfocus.com/bid/56842
url: http://support.microsoft.com/kb/2779030
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪12-078
dfn-cert: DFN-CERT-2012-2237
```

High (CVSS: 10.0)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4571729)

Summary
This host is missing a critical security update according to Microsoft KB4571729

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24559
File checked:      C:\Windows\system32\Ntoskrnl.exe
File version:      6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code, elevate privileges and disclose sensitive information.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An error when the Windows Print Spooler service improperly allows arbitrary writing to the file system.
- An error when the Windows Kernel API fails to properly handle registry objects in memory.
- An error when Windows Media Foundation fails to properly handle objects in memory.
- An error in the way that the scripting engine handles objects in the memory in Internet Explorer.
- An error in RPC if the server has Routing and Remote Access enabled.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4571729)`
OID:1.3.6.1.4.1.25623.1.0.817267
Version used: `2024-06-26T05:05:39Z`

References

```
cve: CVE-2020-1337
cve: CVE-2020-1339
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-1377
cve: CVE-2020-1378
cve: CVE-2020-1379
cve: CVE-2020-1380
cve: CVE-2020-1383
cve: CVE-2020-1464
cve: CVE-2020-1467
cve: CVE-2020-1470
cve: CVE-2020-1472
cve: CVE-2020-1473
cve: CVE-2020-1474
cve: CVE-2020-1475
cve: CVE-2020-1477
cve: CVE-2020-1478
cve: CVE-2020-1484
cve: CVE-2020-1485
cve: CVE-2020-1486
cve: CVE-2020-1489
cve: CVE-2020-1513
cve: CVE-2020-1515
cve: CVE-2020-1516
cve: CVE-2020-1517
cve: CVE-2020-1518
cve: CVE-2020-1519
cve: CVE-2020-1520
cve: CVE-2020-1529
cve: CVE-2020-1530
cve: CVE-2020-1534
cve: CVE-2020-1535
cve: CVE-2020-1536
cve: CVE-2020-1537
cve: CVE-2020-1538
cve: CVE-2020-1539
cve: CVE-2020-1540
cve: CVE-2020-1541
cve: CVE-2020-1542
cve: CVE-2020-1543
cve: CVE-2020-1544
cve: CVE-2020-1545
cve: CVE-2020-1546
cve: CVE-2020-1547
cve: CVE-2020-1551
cve: CVE-2020-1552
cve: CVE-2020-1554
cve: CVE-2020-1557
cve: CVE-2020-1558
cve: CVE-2020-1562
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-1564
cve: CVE-2020-1567
cve: CVE-2020-1570
cve: CVE-2020-1577
cve: CVE-2020-1579
cve: CVE-2020-1584
cve: CVE-2020-1587
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4571729
cert-bund: CB-K21/0411
cert-bund: CB-K20/0816
cert-bund: CB-K20/0814
dfn-cert: DFN-CERT-2020-2749
dfn-cert: DFN-CERT-2020-2567
dfn-cert: DFN-CERT-2020-2024
dfn-cert: DFN-CERT-2020-1775
dfn-cert: DFN-CERT-2020-1768
```

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Summary

This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Community Edition
- Greenbone Enterprise TRIAL (formerly Greenbone Security Manager TRIAL / Greenbone Community Edition VM)
used for this scan.
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Vulnerability Detection Result

```
Version of installed component:          22.4.1 (Installed component: openvas-l
↪ibraries on OpenVAS <= 9, openvas-scanner on Greenbone Community Edition >= 10
↪)
Latest available openvas-scanner version: 23.0.1 (Minimum recommended version, t
↪here are more recent available)
Reference URL(s) for the latest available version: https://forum.greenbone.net/t
↪/greenbone-community-edition-22-4-stable-initial-release-2022-07-25/12638
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Update to the latest available stable release for your scan environment.
Note: It is NOT enough to only update the scanner component. All components should be updated to the most recent and stable versions.
Possible solution options depends on the installation method:
- If using the Greenbone Enterprise TRIAL: Please do a new installation with the newest available version
- If using the official Greenbone Community Containers: Please see the references on how to do an update of these
- If the Greenbone Community Edition was build from sources by following the official source build documentation: Please see the references on how to do an update of all components
- If using packages provided by your Linux distribution: Please contact the maintainer of the used distribution / repository and request updated packages
- If using any other installation method: Please contact the provider of this solution
Please check the references for more information.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked GSM manual.

Vulnerability Detection Method
Details: `Report outdated / end-of-life Scan Engine / Environment (local)`
OID:1.3.6.1.4.1.25623.1.0.108560
Version used: `2024-06-20T05:05:33Z`

References

```
url: https://www.greenbone.net/en/testnow/
url: https://greenbone.github.io/docs/latest/22.4/container/workflows.html#updat
↪ing-the-greenbone-community-containers
url: https://greenbone.github.io/docs/latest/22.4/source-build/workflows.html#up
↪dating-to-newer-releases
url: https://forum.greenbone.net/t/greenbone-community-edition-22-4-stable-initi
↪al-release-2022-07-25/12638
url: https://forum.greenbone.net/t/greenbone-community-edition-21-04-end-of-life
↪/13837
url: https://forum.greenbone.net/t/gvm-21-04-end-of-life-initial-release-2021-04
↪-16/8942
url: https://forum.greenbone.net/t/gvm-20-08-end-of-life-initial-release-2020-08
↪-12/6312
url: https://forum.greenbone.net/t/gvm-11-end-of-life-initial-release-2019-10-14
↪/3674
url: https://forum.greenbone.net/t/gvm-10-end-of-life-initial-release-2019-04-05
↪/208
url: https://forum.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-03-07/
↪211
url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/reports.html#creating-an
↪-override
```

High (CVSS: 10.0)
NVT: Microsoft Windows Networking Components Remote Code Execution Vulnerabilities (2733594)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-054.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to execute arbitrary code on an affected system or cause denial of service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
The flaws are due to
- The way windows networking components handle a specially crafted RAP response.
- A format string error within the print spooler service can be exploited via a specially crafted response.

Vulnerability Detection Method
Details: `Microsoft Windows Networking Components Remote Code Execution Vulnerabilities (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903036
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2012-1850
cve: CVE-2012-1851
cve: CVE-2012-1852
cve: CVE-2012-1853
url: http://support.microsoft.com/kb/2705219
url: http://www.securityfocus.com/bid/54921
url: http://www.securityfocus.com/bid/54928
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/54931
url: http://www.securityfocus.com/bid/54940
url: http://support.microsoft.com/kb/2712808
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-054
dfn-cert: DFN-CERT-2012-1572
```

High (CVSS: 10.0)
NVT: Apache Log4j End of Life (EOL) Detection - Windows

Summary
The Apache Log4j version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result

```
The "Apache Log4j" version on the remote host has reached the end of life.
CPE:               cpe:/a:apache:log4j:1.2.15
Installed version: 1.2.15
Location/URL:      C:\ManageEngine\DesktopCentral_Server\lib\log4j-1.2.15.jar
EOL version:       1.2
EOL date:          2015-08-05
EOL info:          https://blogs.apache.org/foundation/entry/apache_logging_serv
↪ices_project_announces
```

Impact
An EOL version of Apache Log4j is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix
Update the Apache Log4j version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: `Apache Log4j End of Life (EOL) Detection - Windows`
OID:1.3.6.1.4.1.25623.1.0.117844
Version used: `2021-12-17T14:24:48Z`

References

```
url: https://blogs.apache.org/foundation/entry/apache_logging_services_project_a
↪nnounces
```

High (CVSS: 10.0)
NVT: Microsoft Comctl32 Integer Overflow Vulnerability (2864058)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS13-083.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to execute arbitrary code on the system with elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 for x64 Service Pack 1 and prior

Vulnerability Insight
A flaw exists in Comctl32.dll file which is caused by an integer overflow in the common control library.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Comctl32 Integer Overflow Vulnerability (2864058)`
OID:1.3.6.1.4.1.25623.1.0.903225
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2013-3195
url: http://xforce.iss.net/xforce/xfdb/87402
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-083
url: http://support.microsoft.com/default.aspx?scid=kb;EN-US;2864058
cert-bund: CB-K13/0762
dfn-cert: DFN-CERT-2013-1753
```

High (CVSS: 10.0)
NVT: Apache Log4j End of Life (EOL) Detection - Windows

Summary
The Apache Log4j version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result

```
The "Apache Log4j" version on the remote host has reached the end of life.
CPE:                cpe:/a:apache:log4j:1.2.17
Installed version:  1.2.17
Location/URL:       C:\Program Files\elasticsearch-1.1.1\lib\log4j-1.2.17.jar
EOL version:        1.2
EOL date:           2015-08-05
EOL info:           https://blogs.apache.org/foundation/entry/apache_logging_serv
↪ices_project_announces
```

Impact
An EOL version of Apache Log4j is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix
Update the Apache Log4j version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: `Apache Log4j End of Life (EOL) Detection - Windows`
OID:1.3.6.1.4.1.25623.1.0.117844
Version used: `2021-12-17T14:24:48Z`

References

```
url: https://blogs.apache.org/foundation/entry/apache_logging_services_project_a
↪nnounces
```

High (CVSS: 9.9)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5003233)

Summary
This host is missing a critical security update according to Microsoft KB5003233

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24598
File checked:       C:\Windows\system32\Win32k.sys
File version:       6.1.7601.17514
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow an attacker to perform remote code execution, gain access to potentially sensitive data, conduct spoofing and elevate privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- A memory corruption error in Scripting Engine.
- Multiple errors in Windows Remote Desktop Protocol and Microsoft Windows Infrared Data Association.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5003233)`

OID:1.3.6.1.4.1.25623.1.0.818111

Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2020-24587
cve: CVE-2020-24588
cve: CVE-2020-26144
cve: CVE-2021-26419
cve: CVE-2021-28455
cve: CVE-2021-28476
cve: CVE-2021-31182
cve: CVE-2021-31184
cve: CVE-2021-31186
cve: CVE-2021-31188
cve: CVE-2021-31193
cve: CVE-2021-31194
url: https://support.microsoft.com/en-us/help/5003233
cert-bund: WID-SEC-2022-2069
cert-bund: CB-K21/1032
cert-bund: CB-K21/0519
cert-bund: CB-K21/0513
cert-bund: CB-K21/0512
cert-bund: CB-K21/0504
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-0516
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-0737
dfn-cert: DFN-CERT-2023-0393
dfn-cert: DFN-CERT-2023-0324
dfn-cert: DFN-CERT-2022-0633
```

High (CVSS: 9.9)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5005088)

Summary
This host is missing a critical security update according to Microsoft KB5005088

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.25685
File checked:      C:\Windows\system32\spoolsv.exe
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to perform remote code execution, gain access to potentially sensitive data, conduct spoofing and elevate privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An elevation of privilege vulnerability in Windows Common Log File System Driver.
- A security feature bypass vulnerability in Kerberos AppContainer.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5005088)`
OID:1.3.6.1.4.1.25623.1.0.817744
Version used: `2024-01-01T05:05:52Z`

References

```
cve: CVE-2021-26424
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2021-26425
cve: CVE-2021-34480
cve: CVE-2021-34483
cve: CVE-2021-34484
cve: CVE-2021-34533
cve: CVE-2021-34535
cve: CVE-2021-34537
cve: CVE-2021-36927
cve: CVE-2021-36936
cve: CVE-2021-36937
cve: CVE-2021-36942
cve: CVE-2021-36947
cve: CVE-2021-34481
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5005088
cert-bund: CB-K21/0853
cert-bund: CB-K21/0759
```

High (CVSS: 9.9)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4556836)

Summary
This host is missing a critical security update according to Microsoft KB4556836

Vulnerability Detection Result

```
Vulnerable range:  Less than 11.0.9600.19699
File checked:      C:\Windows\system32\Mshtml.dll
File version:      8.0.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code, obtain information to further compromise the user's system, gain elevated privileges and break out of the Edge AppContainer sandbox and run processes in an elevated context.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple flaws exist in Microsoft Scripting Engine, Windows Input and Composition, Windows Media, Windows Storage and Filesystems, and Windows Server.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4556836)`
OID:1.3.6.1.4.1.25623.1.0.817018
Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2020-1010
cve: CVE-2020-1048
cve: CVE-2020-1051
cve: CVE-2020-1112
cve: CVE-2020-1113
cve: CVE-2020-1114
cve: CVE-2020-1153
cve: CVE-2020-1150
cve: CVE-2020-1154
cve: CVE-2020-1054
cve: CVE-2020-1072
cve: CVE-2020-1067
cve: CVE-2020-1071
cve: CVE-2020-1070
cve: CVE-2020-1078
cve: CVE-2020-1179
cve: CVE-2020-0909
cve: CVE-2020-0963
cve: CVE-2020-1116
cve: CVE-2020-1143
cve: CVE-2020-1141
cve: CVE-2020-1061
cve: CVE-2020-1081
cve: CVE-2020-1174
cve: CVE-2020-1175
cve: CVE-2020-1176
cve: CVE-2020-1035
cve: CVE-2020-1060
cve: CVE-2020-1062
cve: CVE-2020-1093
cve: CVE-2020-1058
cve: CVE-2020-1092
cve: CVE-2020-1064
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4556836
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K20/0464
cert-bund: CB-K20/0463
dfn-cert: DFN-CERT-2020-1004
dfn-cert: DFN-CERT-2020-1002
```

High (CVSS: 9.9)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4525235)

Summary
This host is missing a critical security update according to Microsoft KB4525235

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24535
File checked:      C:\Windows\system32\Advapi32.dll
File version:      6.1.7600.16385
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code on a victim system, cause a target system to stop responding, obtain information to further compromise the user's system and gain elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- Windows improperly handles objects in memory.
- Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system.
- Windows kernel improperly handles objects in memory.
- ActiveX Installer service may allow access to files without proper authentication.
- Windows Certificate Dialog does not properly enforce user privileges.
- VBScript engine improperly handles objects in memory.
- The Win32k component fails to properly handle objects in memory.
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4525235)`
OID:1.3.6.1.4.1.25623.1.0.815839

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2023-10-27T16:11:32Z

References

```
cve: CVE-2018-12207
cve: CVE-2019-0712
cve: CVE-2019-0719
cve: CVE-2019-11135
cve: CVE-2019-1382
cve: CVE-2019-1384
cve: CVE-2019-1388
cve: CVE-2019-1389
cve: CVE-2019-1390
cve: CVE-2019-1391
cve: CVE-2019-1393
cve: CVE-2019-1394
cve: CVE-2019-1395
cve: CVE-2019-1396
cve: CVE-2019-1397
cve: CVE-2019-1399
cve: CVE-2019-1405
cve: CVE-2019-1406
cve: CVE-2019-1407
cve: CVE-2019-1408
cve: CVE-2019-1409
cve: CVE-2019-1411
cve: CVE-2019-1412
cve: CVE-2019-1415
cve: CVE-2019-1418
cve: CVE-2019-1419
cve: CVE-2019-1422
cve: CVE-2019-1424
cve: CVE-2019-1429
cve: CVE-2019-1432
cve: CVE-2019-1433
cve: CVE-2019-1434
cve: CVE-2019-1435
cve: CVE-2019-1438
cve: CVE-2019-1439
cve: CVE-2019-1441
cve: CVE-2019-1456
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4525235
cert-bund: WID-SEC-2023-1689
cert-bund: WID-SEC-2023-0884
cert-bund: CB-K20/0691
cert-bund: CB-K19/0986
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K19/0980
cert-bund: CB-K19/0978
dfn-cert: DFN-CERT-2020-1711
dfn-cert: DFN-CERT-2020-1538
dfn-cert: DFN-CERT-2020-1500
dfn-cert: DFN-CERT-2020-0466
dfn-cert: DFN-CERT-2020-0333
dfn-cert: DFN-CERT-2020-0269
dfn-cert: DFN-CERT-2020-0253
dfn-cert: DFN-CERT-2020-0078
dfn-cert: DFN-CERT-2020-0069
dfn-cert: DFN-CERT-2019-2644
dfn-cert: DFN-CERT-2019-2640
dfn-cert: DFN-CERT-2019-2582
dfn-cert: DFN-CERT-2019-2568
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2461
dfn-cert: DFN-CERT-2019-2450
dfn-cert: DFN-CERT-2019-2444
dfn-cert: DFN-CERT-2019-2421
dfn-cert: DFN-CERT-2019-2415
dfn-cert: DFN-CERT-2019-2407
dfn-cert: DFN-CERT-2019-2402
dfn-cert: DFN-CERT-2019-2399
dfn-cert: DFN-CERT-2019-2397
dfn-cert: DFN-CERT-2019-2392
dfn-cert: DFN-CERT-2019-2390
dfn-cert: DFN-CERT-2019-2389
dfn-cert: DFN-CERT-2019-2388
dfn-cert: DFN-CERT-2019-2387
dfn-cert: DFN-CERT-2019-2386
dfn-cert: DFN-CERT-2019-2385
dfn-cert: DFN-CERT-2019-2384
dfn-cert: DFN-CERT-2019-2383
dfn-cert: DFN-CERT-2019-2382
dfn-cert: DFN-CERT-2019-2381
dfn-cert: DFN-CERT-2019-2379
dfn-cert: DFN-CERT-2019-2378
dfn-cert: DFN-CERT-2019-2375
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-2372
dfn-cert: DFN-CERT-2019-2371
dfn-cert: DFN-CERT-2019-2370
dfn-cert: DFN-CERT-2019-2368
```

High (CVSS: 9.9)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4499164)

Summary
This host is missing a critical security update according to Microsoft KB4499164.

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24441
File checked:      C:\Windows\system32\Ntdll.dll
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code on a victim system, obtain information to further compromise the user's system, gain elevated privileges, conduct remote code execution and conduct spoofing attack.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist as,
- Windows Jet Database Engine improperly handles objects in memory.
- Windows Graphics Device Interface (GDI) improperly handles objects in the memory.
- Internet Explorer improperly handles URLs.
- Windows fails to properly handle certain symbolic links.
- An error Active Directory Forest trusts due to a default setting.
- Windows Server DHCP service improperly process specially crafted packets.
- Remote Code Execution Vulnerability in Windows Remote Desktop Service (Bluekeep).
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4499164)`
OID:1.3.6.1.4.1.25623.1.0.815051
Version used: `2023-10-27T16:11:32Z`

References

```
cve: CVE-2018-11091
cve: CVE-2018-12126
cve: CVE-2018-12127
cve: CVE-2018-12130
cve: CVE-2019-0683
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2019-0708
cve: CVE-2019-0725
cve: CVE-2019-0734
cve: CVE-2019-0758
cve: CVE-2019-0863
cve: CVE-2019-0881
cve: CVE-2019-0882
cve: CVE-2019-0884
cve: CVE-2019-0885
cve: CVE-2019-0889
cve: CVE-2019-0890
cve: CVE-2019-0891
cve: CVE-2019-0893
cve: CVE-2019-0894
cve: CVE-2019-0895
cve: CVE-2019-0896
cve: CVE-2019-0897
cve: CVE-2019-0898
cve: CVE-2019-0899
cve: CVE-2019-0900
cve: CVE-2019-0901
cve: CVE-2019-0902
cve: CVE-2019-0903
cve: CVE-2019-0911
cve: CVE-2019-0918
cve: CVE-2019-0921
cve: CVE-2019-0930
cve: CVE-2019-0936
cve: CVE-2019-0940
cve: CVE-2019-0961
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4499164
cert-bund: WID-SEC-2023-1692
cert-bund: CB-K19/0422
cert-bund: CB-K19/0421
cert-bund: CB-K19/0415
cert-bund: CB-K19/0414
cert-bund: CB-K19/0212
cert-bund: CB-K19/0005
dfn-cert: DFN-CERT-2020-1041
dfn-cert: DFN-CERT-2020-0069
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-2214
dfn-cert: DFN-CERT-2019-1985
dfn-cert: DFN-CERT-2019-1767
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-1414
dfn-cert: DFN-CERT-2019-1235
dfn-cert: DFN-CERT-2019-1200
dfn-cert: DFN-CERT-2019-1172
dfn-cert: DFN-CERT-2019-1151
dfn-cert: DFN-CERT-2019-1149
dfn-cert: DFN-CERT-2019-1122
dfn-cert: DFN-CERT-2019-1083
dfn-cert: DFN-CERT-2019-1036
dfn-cert: DFN-CERT-2019-1032
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-1025
dfn-cert: DFN-CERT-2019-1024
dfn-cert: DFN-CERT-2019-1017
dfn-cert: DFN-CERT-2019-1012
dfn-cert: DFN-CERT-2019-1009
dfn-cert: DFN-CERT-2019-1005
dfn-cert: DFN-CERT-2019-1004
dfn-cert: DFN-CERT-2019-1003
dfn-cert: DFN-CERT-2019-1002
dfn-cert: DFN-CERT-2019-0994
dfn-cert: DFN-CERT-2019-0990
dfn-cert: DFN-CERT-2019-0989
dfn-cert: DFN-CERT-2019-0988
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0986
dfn-cert: DFN-CERT-2019-0977
dfn-cert: DFN-CERT-2019-0975
dfn-cert: DFN-CERT-2019-0974
dfn-cert: DFN-CERT-2019-0971
dfn-cert: DFN-CERT-2019-0969
dfn-cert: DFN-CERT-2019-0965
dfn-cert: DFN-CERT-2019-0961
dfn-cert: DFN-CERT-2019-0950
dfn-cert: DFN-CERT-2019-0506
dfn-cert: DFN-CERT-2018-2399
```

High (CVSS: 9.9)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4519976)

Summary
This host is missing a critical security update according to Microsoft KB4519976

Vulnerability Detection Result

```
Vulnerable range:   Less than 11.0.9600.19507
File checked:       C:\Windows\system32\Mshtml.dll
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
File version:      8.0.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code on a victim system, obtain information to further compromise the user's system, gain elevated privileges and disclose sensitive information or cause denial of service.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- Improper parsing of HTTP content.
- Improper handling of objects in memory in VBScript engine.
- Improperly handling of hard links in Windows Error Reporting manager.
- Improper handling of a Registry Restore Key function in 'umpo.dll' of Power Service.
- Improper handling of process crash in Windows Error Reporting manager.
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4519976)`
OID:1.3.6.1.4.1.25623.1.0.815710
Version used: 2023-10-27T16:11:32Z

References
cve: CVE-2019-0608
cve: CVE-2019-1166
cve: CVE-2019-1192
cve: CVE-2019-1238
cve: CVE-2019-1315
cve: CVE-2019-1318
cve: CVE-2019-1319
cve: CVE-2019-1325
cve: CVE-2019-1326
cve: CVE-2019-1333
cve: CVE-2019-1338
cve: CVE-2019-1339
cve: CVE-2019-1341
cve: CVE-2019-1342
cve: CVE-2019-1344

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2019-1346
cve: CVE-2019-1357
cve: CVE-2019-1358
cve: CVE-2019-1359
cve: CVE-2019-1361
cve: CVE-2019-1362
cve: CVE-2019-1363
cve: CVE-2019-1364
cve: CVE-2019-1365
cve: CVE-2019-1367
cve: CVE-2019-1371
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4519976
cert-bund: CB-K19/0892
cert-bund: CB-K19/0888
cert-bund: CB-K19/0885
cert-bund: CB-K19/0833
cert-bund: CB-K19/0789
cert-bund: CB-K19/0788
dfn-cert: DFN-CERT-2019-2107
dfn-cert: DFN-CERT-2019-2103
dfn-cert: DFN-CERT-2019-2101
dfn-cert: DFN-CERT-2019-1979
dfn-cert: DFN-CERT-2019-1711
dfn-cert: DFN-CERT-2019-1708
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5017361)

Summary
This host is missing an important security update according to Microsoft KB5017361

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.26111
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
- Microsoft Windows 7 for 32-bit Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- A Remote Code Execution Vulnerability in Windows Internet Key Exchange (IKE) Protocol Extensions.
- An elevation of privilege vulnerability in Windows Common Log File System Driver.
- A Denial of Service Vulnerability in Windows DNS Server.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5017361)`
OID:1.3.6.1.4.1.25623.1.0.826448
Version used: `2023-10-19T05:05:21Z`

References
```
cve: CVE-2022-26929
cve: CVE-2022-30170
cve: CVE-2022-30200
cve: CVE-2022-33647
cve: CVE-2022-33679
cve: CVE-2022-34718
cve: CVE-2022-34719
cve: CVE-2022-34720
cve: CVE-2022-34721
cve: CVE-2022-34722
cve: CVE-2022-34724
cve: CVE-2022-34726
cve: CVE-2022-34727
cve: CVE-2022-34728
cve: CVE-2022-34729
cve: CVE-2022-34730
cve: CVE-2022-34731
cve: CVE-2022-34732
cve: CVE-2022-34733
cve: CVE-2022-34734
cve: CVE-2022-35803
cve: CVE-2022-35830
cve: CVE-2022-35832
cve: CVE-2022-35833
cve: CVE-2022-35834
cve: CVE-2022-35835
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2022-35836
cve: CVE-2022-35837
cve: CVE-2022-35840
cve: CVE-2022-37955
cve: CVE-2022-37956
cve: CVE-2022-37958
cve: CVE-2022-37964
cve: CVE-2022-37969
cve: CVE-2022-38004
cve: CVE-2022-38005
cve: CVE-2022-38006
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5017361
cert-bund: WID-SEC-2022-1406
cert-bund: WID-SEC-2022-1403
dfn-cert: DFN-CERT-2022-2028
dfn-cert: DFN-CERT-2022-2022
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5016676)

Summary
This host is missing an important security update according to Microsoft KB5016676

Vulnerability Detection Result

```
Vulnerable range:   6.1.7601.0 - 6.1.7601.26062
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:

. . . continues on next page . . .

. . . continued from previous page . . .

- An elevation of privilege vulnerability in Active Directory Domain Services.
- A Remote Code Execution Vulnerability in Windows Point-to-Point Protocol.
- A Denial of Service Vulnerability in Windows Point-to-Point Protocol.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5016676)`
OID:1.3.6.1.4.1.25623.1.0.817790
Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-30133
cve: CVE-2022-30194
cve: CVE-2022-34690
cve: CVE-2022-34691
cve: CVE-2022-34701
cve: CVE-2022-34702
cve: CVE-2022-34706
cve: CVE-2022-34707
cve: CVE-2022-34708
cve: CVE-2022-34713
cve: CVE-2022-34714
cve: CVE-2022-35743
cve: CVE-2022-35744
cve: CVE-2022-35745
cve: CVE-2022-35747
cve: CVE-2022-35750
cve: CVE-2022-35751
cve: CVE-2022-35752
cve: CVE-2022-35753
cve: CVE-2022-35756
cve: CVE-2022-35758
cve: CVE-2022-35759
cve: CVE-2022-35760
cve: CVE-2022-35767
cve: CVE-2022-35768
cve: CVE-2022-35769
cve: CVE-2022-35793
cve: CVE-2022-35795
cve: CVE-2022-35820
cve: CVE-2022-34689
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5016676
cert-bund: WID-SEC-2022-1682
cert-bund: WID-SEC-2022-1251
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0957
dfn-cert: DFN-CERT-2022-2249
dfn-cert: DFN-CERT-2022-1784
```

High (CVSS: 9.8)
NVT: Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check

Summary
Apache Log4j is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.2.15
Fixed version:     None
Installation
path / port:       C:\Program Files\Apache Software Foundation\tomcat\apache-tom
↪cat-8.0.33\webapps\axis2\WEB-INF\lib\log4j-1.2.15.jar
```

Solution:
Solution type: WillNotFix
No solution was made available by the vendor.
Note: Apache Log4j 1.x reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Affected Software/OS
Apache Log4j version 1.x.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-23302: Deserialization of untrusted data in JMSSink. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default.
- CVE-2022-23305: SQL injection in JDBC Appender. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default.
- CVE-2022-23307/CVE-2020-9493: A deserialization flaw in the Chainsaw component of Log4j 1.x can lead to malicious code execution.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check`
OID:1.3.6.1.4.1.25623.1.0.117902
Version used: `2023-10-18T05:05:17Z`

References

```
cve: CVE-2022-23302
cve: CVE-2022-23305
cve: CVE-2022-23307
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-9493
url: https://www.openwall.com/lists/oss-security/2022/01/18/3
url: https://www.openwall.com/lists/oss-security/2022/01/18/4
url: https://www.openwall.com/lists/oss-security/2022/01/18/5
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-1809
cert-bund: WID-SEC-2023-1027
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1909
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1780
cert-bund: WID-SEC-2022-1778
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1769
cert-bund: WID-SEC-2022-0754
cert-bund: WID-SEC-2022-0752
cert-bund: WID-SEC-2022-0738
cert-bund: WID-SEC-2022-0521
cert-bund: WID-SEC-2022-0169
cert-bund: CB-K22/0476
cert-bund: CB-K22/0471
cert-bund: CB-K22/0468
cert-bund: CB-K22/0464
cert-bund: CB-K22/0075
dfn-cert: DFN-CERT-2023-0860
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2311
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-1615
dfn-cert: DFN-CERT-2022-1472
dfn-cert: DFN-CERT-2022-1176
dfn-cert: DFN-CERT-2022-0874
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2022-0305
dfn-cert: DFN-CERT-2022-0292
dfn-cert: DFN-CERT-2022-0290
dfn-cert: DFN-CERT-2022-0204
dfn-cert: DFN-CERT-2022-0203
```

High (CVSS: 9.8)
NVT: Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check

. . . continues on next page . . .

... continued from previous page ...

Summary
Apache Log4j is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.2.15
Fixed version:     None
Installation
path / port:       C:\ManageEngine\DesktopCentral_Server\lib\log4j-1.2.15.jar
```

Solution:
Solution type: WillNotFix
No solution was made available by the vendor.
Note: Apache Log4j 1.x reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Affected Software/OS
Apache Log4j version 1.x.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-23302: Deserialization of untrusted data in JMSSink. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default.
- CVE-2022-23305: SQL injection in JDBC Appender. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default.
- CVE-2022-23307/CVE-2020-9493: A deserialization flaw in the Chainsaw component of Log4j 1.x can lead to malicious code execution.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check`
OID:1.3.6.1.4.1.25623.1.0.117902
Version used: `2023-10-18T05:05:17Z`

References

```
cve: CVE-2022-23302
cve: CVE-2022-23305
cve: CVE-2022-23307
cve: CVE-2020-9493
url: https://www.openwall.com/lists/oss-security/2022/01/18/3
url: https://www.openwall.com/lists/oss-security/2022/01/18/4
url: https://www.openwall.com/lists/oss-security/2022/01/18/5
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-1809
cert-bund: WID-SEC-2023-1027
cert-bund: WID-SEC-2023-0132
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-1909
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1780
cert-bund: WID-SEC-2022-1778
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1769
cert-bund: WID-SEC-2022-0754
cert-bund: WID-SEC-2022-0752
cert-bund: WID-SEC-2022-0738
cert-bund: WID-SEC-2022-0521
cert-bund: WID-SEC-2022-0169
cert-bund: CB-K22/0476
cert-bund: CB-K22/0471
cert-bund: CB-K22/0468
cert-bund: CB-K22/0464
cert-bund: CB-K22/0075
dfn-cert: DFN-CERT-2023-0860
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2311
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-1615
dfn-cert: DFN-CERT-2022-1472
dfn-cert: DFN-CERT-2022-1176
dfn-cert: DFN-CERT-2022-0874
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2022-0305
dfn-cert: DFN-CERT-2022-0292
dfn-cert: DFN-CERT-2022-0290
dfn-cert: DFN-CERT-2022-0204
dfn-cert: DFN-CERT-2022-0203
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5014012)

Summary

This host is missing an important security update according to Microsoft KB5014012

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.25954
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information, bypass security restrictions, conduct spoofing attacks and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An elevation of privilege vulnerability in Windows Kerberos.
- A Remote Code Execution Vulnerability in Windows Network File System.
- A Denial of Service Vulnerability in Windows WLAN AutoConfig Service.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5014012)`
OID:1.3.6.1.4.1.25623.1.0.821111
Version used: `2023-10-19T05:05:21Z`

References
```
cve: CVE-2022-21972
cve: CVE-2022-22011
cve: CVE-2022-22012
cve: CVE-2022-22013
cve: CVE-2022-22014
cve: CVE-2022-22015
cve: CVE-2022-22019
cve: CVE-2022-23270
cve: CVE-2022-26788
cve: CVE-2022-26925
cve: CVE-2022-26926
cve: CVE-2022-26931
cve: CVE-2022-26934
cve: CVE-2022-26935
cve: CVE-2022-26936
cve: CVE-2022-26937
cve: CVE-2022-29103
cve: CVE-2022-29105
cve: CVE-2022-29112
cve: CVE-2022-29115
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2022-29121
cve: CVE-2022-29127
cve: CVE-2022-29128
cve: CVE-2022-29129
cve: CVE-2022-29130
cve: CVE-2022-29132
cve: CVE-2022-29137
cve: CVE-2022-29139
cve: CVE-2022-29141
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5014012
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1176
cert-bund: WID-SEC-2022-0450
cert-bund: CB-K22/0579
cert-bund: CB-K22/0427
dfn-cert: DFN-CERT-2022-1045
dfn-cert: DFN-CERT-2022-1041
dfn-cert: DFN-CERT-2022-0948
dfn-cert: DFN-CERT-2022-0817
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5012626)

Summary
This host is missing an important security update according to Microsoft KB5012626

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.25920
File checked:      C:\Windows\system32\Ntoskrnl.exe
File version:      6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privileges, disclose sensitive information, conduct remote code execution, and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to:
- A remote code execution vulnerability in Windows DNS Server.
- An elevation of privilege vulnerability in Windows Print Spooler.
- An elevation of privilege vulnerability in Windows File Server Resource Management Service.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5012626)`
OID:1.3.6.1.4.1.25623.1.0.820077
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2022-21983
cve: CVE-2022-24474
cve: CVE-2022-24481
cve: CVE-2022-24485
cve: CVE-2022-24492
cve: CVE-2022-24493
cve: CVE-2022-24494
cve: CVE-2022-24498
cve: CVE-2022-24499
cve: CVE-2022-24500
cve: CVE-2022-24521
cve: CVE-2022-24527
cve: CVE-2022-24528
cve: CVE-2022-24530
cve: CVE-2022-24533
cve: CVE-2022-24534
cve: CVE-2022-24536
cve: CVE-2022-24540
cve: CVE-2022-24541
cve: CVE-2022-24542
cve: CVE-2022-24544
cve: CVE-2022-26787
cve: CVE-2022-26790
cve: CVE-2022-26792
cve: CVE-2022-26794
cve: CVE-2022-26796
cve: CVE-2022-26797
cve: CVE-2022-26798
cve: CVE-2022-26801
cve: CVE-2022-26802
cve: CVE-2022-26803
cve: CVE-2022-26807
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2022-26809
cve: CVE-2022-26810
cve: CVE-2022-26812
cve: CVE-2022-26813
cve: CVE-2022-26815
cve: CVE-2022-26819
cve: CVE-2022-26820
cve: CVE-2022-26821
cve: CVE-2022-26822
cve: CVE-2022-26827
cve: CVE-2022-26829
cve: CVE-2022-26831
cve: CVE-2022-26903
cve: CVE-2022-26904
cve: CVE-2022-26915
cve: CVE-2022-26916
cve: CVE-2022-26917
cve: CVE-2022-26918
cve: CVE-2022-26919
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5012626
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-0450
cert-bund: CB-K22/0427
dfn-cert: DFN-CERT-2022-0817
dfn-cert: DFN-CERT-2022-0814
```

High (CVSS: 9.8)
NVT: Microsoft Web Proxy Auto Discovery (WPAD) Privilege Elevation Vulnerabilities (3165191)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-077.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Ws2_32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23451
```

Impact
Successful exploitation will allow an attacker to bypass security and gain elevated privileges on a targeted system, and to potentially access and control network traffic for which the attacker does not have sufficient privileges.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight

Multiple flaws exist due to:

- when the Web Proxy Auto Discovery (WPAD) protocol falls back to a vulnerable proxy discovery process.
- when Microsoft Windows improperly handles certain proxy discovery scenarios using the Web Proxy Auto Discovery (WPAD) protocol method.
- when NetBIOS improperly handles responses.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Web Proxy Auto Discovery (WPAD) Privilege Elevation Vulnerabilities (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.808085

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3213
cve: CVE-2016-3236
cve: CVE-2016-3299
url: https://support.microsoft.com/en-us/kb/3165191
url: http://www.securityfocus.com/bid/91111
url: http://www.securityfocus.com/bid/92387
url: http://www.securityfocus.com/bid/91114
url: https://technet.microsoft.com/en-us/library/security/MS16-077
cert-bund: CB-K16/0914
cert-bund: CB-K16/0901
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5008244)

Summary

This host is missing a critical security update according to Microsoft KB5008244

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.25792
File checked:      C:\Windows\system32\advapi32.dll
File version:      6.1.7600.16385
```

Impact

Successful exploitation will allow an attacker to elevate privileges, disclose sensitive information and conduct remote code execution.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- An elevation of privilege vulnerability in Windows Encrypting File System (EFS).
- An RCE vulnerability in Windows Encrypting File System (EFS).
- A memory corruption vulnerability in iSNS Server.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5008244)`

OID:1.3.6.1.4.1.25623.1.0.818921

Version used: `2021-12-23T12:12:57Z`

References

```
cve: CVE-2021-40441
cve: CVE-2021-41333
cve: CVE-2021-43207
cve: CVE-2021-43215
cve: CVE-2021-43216
cve: CVE-2021-43217
cve: CVE-2021-43222
cve: CVE-2021-43223
cve: CVE-2021-43224
cve: CVE-2021-43226
cve: CVE-2021-43229
cve: CVE-2021-43230
cve: CVE-2021-43233
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2021-43234
cve: CVE-2021-43236
cve: CVE-2021-43238
cve: CVE-2021-43245
cve: CVE-2021-43883
cve: CVE-2021-43893
url: https://support.microsoft.com/en-us/help/5008244
cert-bund: CB-K21/1287
```

High (CVSS: 9.8)
NVT: Microsoft .NET Framework Multiple RCE Vulnerabilities (KB4535102)

Summary
This host is missing a critical security update according to Microsoft KB4535102

Vulnerability Detection Result

```
Vulnerable range:  4.0 - 4.0.30319.36576
File checked:      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.workfl
↪ow.runtime.dll
File version:      4.0.30319.34209
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight
Multiple flaws exist due to:
- Microsoft .NET Framework fails to check the source markup of a file.
- Microsoft .NET Framework fails to validate input properly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Multiple RCE Vulnerabilities (KB4535102)`
OID:1.3.6.1.4.1.25623.1.0.816552
Version used: `2022-08-09T10:11:17Z`

... continues on next page ...

. . . continued from previous page . . .

References

```
cve: CVE-2020-0646
cve: CVE-2020-0605
cve: CVE-2020-0606
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4535102/
cert-bund: CB-K20/0048
dfn-cert: DFN-CERT-2020-0087
```

High (CVSS: 9.8)
NVT: Microsoft .NET Framework 4.5.2 Multiple Vulnerabilities (KB4470637)

Summary
This host is missing a critical security update according to Microsoft KB4470637

Vulnerability Detection Result

```
Vulnerable range:  4.0.30319.30000 - 4.0.30319.36464
File checked:      C:\Windows\Microsoft.NET\Framework64\v2.0.50727webengine.dll
File version:      2.0.50727.5420
```

Impact
Successful exploitation will allow an attacker to cause a denial of service condition and take control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 4.5.2 for Microsoft Windows 7 SP1, Server 2008 R2 SP1, and Microsoft Windows Server 2008 SP2.

Vulnerability Insight
Multiple flaws exist due to:
- An error when .NET Framework improperly handles special web requests.
- An error when the Microsoft .NET Framework fails to validate input properly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework 4.5.2 Multiple Vulnerabilities (KB4470637)`
OID:1.3.6.1.4.1.25623.1.0.814705
Version used: `2023-07-20T05:05:17Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-8517
cve: CVE-2018-8540
url: https://support.microsoft.com/en-us/help/4470637
url: http://www.securityfocus.com/bid/106075
url: http://www.securityfocus.com/bid/106073
cert-bund: CB-K18/1158
dfn-cert: DFN-CERT-2018-2517
```

High (CVSS: 9.8)
NVT: Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows

Summary

Apache Log4j is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.2.17
Fixed version:     2.x
Installation
path / port:       C:\Program Files\elasticsearch-1.1.1\lib\log4j-1.2.17.jar
```

Solution:

Solution type: VendorFix

Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2.x which both addresses that vulnerability as well as numerous other issues in the previous versions.

Affected Software/OS

Apache Log4j versions 1.2.x through 1.2.17.

Vulnerability Insight

Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.117864

Version used: `2021-12-22T14:03:25Z`

References

```
cve: CVE-2019-17571
url: https://lists.apache.org/thread/173yrzw9trfy6xdydfz05tsvp79z8rt7
url: https://issues.apache.org/jira/browse/LOG4J2-1863
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-0138
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0770
cert-bund: WID-SEC-2022-0368
cert-bund: CB-K21/0493
cert-bund: CB-K20/0555
cert-bund: CB-K20/0363
dfn-cert: DFN-CERT-2023-0860
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-0988
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0050
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4601347)

Summary
This host is missing a critical security update according to Microsoft KB4601347

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24565
File checked:      C:\Windows\system32\kernel32.dll
File version:      6.1.7601.17514
```

Impact
Successful exploitation allows an attacker to execute arbitrary code on a victim system, disclose sensitive information, conduct denial-of-service condition and gain elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An error in Windows Fax Service.
- An error in Windows Installer.
- An error in Windows Remote Procedure Call.
- An error in Windows TCP/IP. For more information about the vulnerabilities refer to Reference links.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4601347)`

OID:1.3.6.1.4.1.25623.1.0.817597

Version used: `2021-08-25T12:01:03Z`

References

```
cve: CVE-2021-1722
cve: CVE-2021-1727
cve: CVE-2021-1734
cve: CVE-2021-24074
cve: CVE-2021-24077
cve: CVE-2021-24078
cve: CVE-2021-24080
cve: CVE-2021-24083
cve: CVE-2021-24086
cve: CVE-2021-24088
cve: CVE-2021-24094
cve: CVE-2021-24102
cve: CVE-2021-24103
cve: CVE-2021-25195
url: https://support.microsoft.com/en-us/help/4601347
cert-bund: CB-K21/0153
```

High (CVSS: 9.8)

NVT: Microsoft Windows Multiple Vulnerabilities (KB4586827)

Summary

This host is missing a critical security update according to Microsoft KB4586827

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24562
File checked:       C:\Windows\system32\Kernel32.dll
File version:       6.1.7601.17514
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code, elevate privileges and disclose sensitive information.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- Incorrect processing of user-supplied data in Windows.
- Error in excessive data output by the application in Windows Graphics Component.
- Windows Port Class Library fails to properly impose security restrictions.
- Windows Print Spooler fails to properly impose security restrictions.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4586827)`

OID:1.3.6.1.4.1.25623.1.0.817539

Version used: `2024-06-26T05:05:39Z`

References

```
cve: CVE-2020-1599
cve: CVE-2020-16997
cve: CVE-2020-17000
cve: CVE-2020-17001
cve: CVE-2020-17004
cve: CVE-2020-17011
cve: CVE-2020-17014
cve: CVE-2020-17029
cve: CVE-2020-17036
cve: CVE-2020-17038
cve: CVE-2020-17042
cve: CVE-2020-17043
cve: CVE-2020-17044
cve: CVE-2020-17045
cve: CVE-2020-17047
cve: CVE-2020-17051
cve: CVE-2020-17052
cve: CVE-2020-17068
cve: CVE-2020-17069
cve: CVE-2020-17087
cve: CVE-2020-17088
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4586827
cert-bund: CB-K20/1111
cert-bund: CB-K20/1109
cert-bund: CB-K20/1108
cert-bund: CB-K20/1056
dfn-cert: DFN-CERT-2020-2467
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2465
dfn-cert: DFN-CERT-2020-2464
```

High (CVSS: 9.8)
NVT: Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows

Summary
Apache Log4j is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.2.17
Fixed version:     2.x
Installation
path / port:       C:\Program Files\Apache Software Foundation\tomcat\apache-tom
↪cat-8.0.33\webapps\struts2-rest-showcase\WEB-INF\lib\log4j-1.2.17.jar
```

Solution:
Solution type: VendorFix
Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2.x which both addresses that vulnerability as well as numerous other issues in the previous versions.

Affected Software/OS
Apache Log4j versions 1.2.x through 1.2.17.

Vulnerability Insight
Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.117864
Version used: 2021-12-22T14:03:25Z

References

```
cve: CVE-2019-17571
url: https://lists.apache.org/thread/173yrzw9trfy6xdydfz05tsvp79z8rt7
url: https://issues.apache.org/jira/browse/LOG4J2-1863
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-0138
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0770
cert-bund: WID-SEC-2022-0368
cert-bund: CB-K21/0493
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K20/0555
cert-bund: CB-K20/0363
dfn-cert: DFN-CERT-2023-0860
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-0988
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0050
```

High (CVSS: 9.8)
NVT: Oracle Java SE Security Update (Apr 2024) -02 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation allows an attacker to compromise Oracle Java SE, which can result in unauthorized update, insert or delete access to some of Oracle Java SE.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE 8u401 and prior on Windows.

Vulnerability Insight
These vulnerabilities exist:
- CVE-2024-21003: An error in the JavaFX component of Oracle Java SE.
- CVE-2024-21005: An error in the JavaFX component of Oracle Java SE.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (Apr 2024) -02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832953
Version used: `2024-04-26T15:38:47Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2023-41993
cve: CVE-2024-21003
cve: CVE-2024-21005
cve: CVE-2024-21002
cve: CVE-2024-21004
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://www.oracle.com/security-alerts/cpuapr2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-0895
cert-bund: WID-SEC-2023-2705
cert-bund: WID-SEC-2023-2454
cert-bund: WID-SEC-2023-2453
cert-bund: WID-SEC-2023-2452
cert-bund: WID-SEC-2023-2427
cert-bund: WID-SEC-2023-2424
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1005
dfn-cert: DFN-CERT-2024-1004
dfn-cert: DFN-CERT-2023-2645
dfn-cert: DFN-CERT-2023-2334
dfn-cert: DFN-CERT-2023-2333
dfn-cert: DFN-CERT-2023-2297
dfn-cert: DFN-CERT-2023-2296
dfn-cert: DFN-CERT-2023-2246
dfn-cert: DFN-CERT-2023-2245
```

High (CVSS: 9.8)
NVT: Oracle Java SE Security Update (Apr 2024) -02 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation allows an attacker to compromise Oracle Java SE, which can result in unauthorized update, insert or delete access to some of Oracle Java SE.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle Java SE 8u401 and prior on Windows.

Vulnerability Insight
These vulnerabilities exist:
- CVE-2024-21003: An error in the JavaFX component of Oracle Java SE.
- CVE-2024-21005: An error in the JavaFX component of Oracle Java SE.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (Apr 2024) -02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832953
Version used: `2024-04-26T15:38:47Z`

References

```
cve: CVE-2023-41993
cve: CVE-2024-21003
cve: CVE-2024-21005
cve: CVE-2024-21002
cve: CVE-2024-21004
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://www.oracle.com/security-alerts/cpuapr2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-0895
cert-bund: WID-SEC-2023-2705
cert-bund: WID-SEC-2023-2454
cert-bund: WID-SEC-2023-2453
cert-bund: WID-SEC-2023-2452
cert-bund: WID-SEC-2023-2427
cert-bund: WID-SEC-2023-2424
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1005
dfn-cert: DFN-CERT-2024-1004
dfn-cert: DFN-CERT-2023-2645
dfn-cert: DFN-CERT-2023-2334
dfn-cert: DFN-CERT-2023-2333
dfn-cert: DFN-CERT-2023-2297
dfn-cert: DFN-CERT-2023-2296
dfn-cert: DFN-CERT-2023-2246
dfn-cert: DFN-CERT-2023-2245
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4512506)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing a critical security update according to Microsoft KB4512506.

Vulnerability Detection Result

```
Vulnerable range:  Less than 11.0.9600.19431
File checked:      C:\Windows\system32\Urlmon.dll
File version:      8.0.7601.17514
```

Impact
Successful exploitation will allow an attacker to crash the host server, execute arbitrary code on the target system, obtain information that could be used to try to further compromise the affected system and negotiate the offered key length of bluetooth connection.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist as,
- Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system.
- Windows improperly handles objects in memory.
- VBScript engine improperly handles objects in memory.
- The XmlLite runtime (XmlLite.dll) improperly parses XML input.
- Microsoft browsers improperly handle requests of different origins.
- Windows Server DHCP service improperly process specially crafted packets.
- Bluetooth BR/EDR key negotiation vulnerability that exists at the hardware specification level of any BR/EDR Bluetooth device.
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4512506)`
OID:1.3.6.1.4.1.25623.1.0.815438
Version used: `2024-05-30T05:05:32Z`

References

```
cve: CVE-2019-0714
cve: CVE-2019-0715
cve: CVE-2019-0716
cve: CVE-2019-0720
cve: CVE-2019-0723
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2019-0736
cve: CVE-2019-1057
cve: CVE-2019-1078
cve: CVE-2019-1133
cve: CVE-2019-1143
cve: CVE-2019-1144
cve: CVE-2019-1145
cve: CVE-2019-1146
cve: CVE-2019-1147
cve: CVE-2019-1148
cve: CVE-2019-1149
cve: CVE-2019-1150
cve: CVE-2019-1151
cve: CVE-2019-1152
cve: CVE-2019-1153
cve: CVE-2019-1154
cve: CVE-2019-1155
cve: CVE-2019-1156
cve: CVE-2019-1157
cve: CVE-2019-1158
cve: CVE-2019-1159
cve: CVE-2019-1162
cve: CVE-2019-1164
cve: CVE-2019-1168
cve: CVE-2019-1169
cve: CVE-2019-1177
cve: CVE-2019-1178
cve: CVE-2019-1181
cve: CVE-2019-1182
cve: CVE-2019-1183
cve: CVE-2019-1187
cve: CVE-2019-1192
cve: CVE-2019-1193
cve: CVE-2019-1194
cve: CVE-2019-1212
cve: CVE-2019-1228
cve: CVE-2019-9506
url: https://support.microsoft.com/en-us/help/4512506
cert-bund: CB-K20/0326
cert-bund: CB-K19/0789
cert-bund: CB-K19/0788
cert-bund: CB-K19/0733
cert-bund: CB-K19/0725
cert-bund: CB-K19/0720
cert-bund: CB-K19/0649
cert-bund: CB-K19/0644
dfn-cert: DFN-CERT-2020-0861
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0078
dfn-cert: DFN-CERT-2019-2640
dfn-cert: DFN-CERT-2019-2582
dfn-cert: DFN-CERT-2019-2421
dfn-cert: DFN-CERT-2019-2389
dfn-cert: DFN-CERT-2019-2388
dfn-cert: DFN-CERT-2019-2313
dfn-cert: DFN-CERT-2019-2269
dfn-cert: DFN-CERT-2019-2247
dfn-cert: DFN-CERT-2019-2246
dfn-cert: DFN-CERT-2019-2217
dfn-cert: DFN-CERT-2019-2204
dfn-cert: DFN-CERT-2019-2167
dfn-cert: DFN-CERT-2019-2132
dfn-cert: DFN-CERT-2019-2125
dfn-cert: DFN-CERT-2019-2096
dfn-cert: DFN-CERT-2019-2076
dfn-cert: DFN-CERT-2019-1994
dfn-cert: DFN-CERT-2019-1933
dfn-cert: DFN-CERT-2019-1828
dfn-cert: DFN-CERT-2019-1825
dfn-cert: DFN-CERT-2019-1711
dfn-cert: DFN-CERT-2019-1708
dfn-cert: DFN-CERT-2019-1691
dfn-cert: DFN-CERT-2019-1689
dfn-cert: DFN-CERT-2019-1512
dfn-cert: DFN-CERT-2019-1511
dfn-cert: DFN-CERT-2019-1157
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5028240)

Summary
This host is missing an important security update according to Microsoft KB5028240

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.26623
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information and conduct DoS attacks.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1.

Vulnerability Insight
Multiple flaws exist due to:
- A Remote Code Execution Vulnerability in Windows Routing and Remote Access Service (RRAS).
- A Remote Code Execution Vulnerability in Microsoft Message Queuing.
- A Remote Code Execution Vulnerability in Windows DNS Server.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5028240)`
OID:1.3.6.1.4.1.25623.1.0.832300
Version used: `2023-10-13T05:06:10Z`

References
```
cve: CVE-2023-35299
cve: CVE-2023-32053
cve: CVE-2023-35366
cve: CVE-2023-33154
cve: CVE-2023-32044
cve: CVE-2023-35367
cve: CVE-2023-32057
cve: CVE-2023-32055
cve: CVE-2023-33169
cve: CVE-2023-36874
cve: CVE-2023-35310
cve: CVE-2023-32054
cve: CVE-2023-35365
cve: CVE-2023-32050
cve: CVE-2023-33168
cve: CVE-2023-35303
cve: CVE-2023-32038
cve: CVE-2023-21526
cve: CVE-2023-35309
cve: CVE-2023-33174
cve: CVE-2023-35351
cve: CVE-2023-35350
cve: CVE-2023-35346
cve: CVE-2023-35345
cve: CVE-2023-35344
cve: CVE-2023-35342
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2023-35341
cve: CVE-2023-35340
cve: CVE-2023-35338
cve: CVE-2023-35332
cve: CVE-2023-35330
cve: CVE-2023-35328
cve: CVE-2023-35322
cve: CVE-2023-35321
cve: CVE-2023-35319
cve: CVE-2023-35318
cve: CVE-2023-35316
cve: CVE-2023-35314
cve: CVE-2023-35312
cve: CVE-2023-35300
cve: CVE-2023-35297
cve: CVE-2023-32046
cve: CVE-2023-32045
cve: CVE-2023-32043
cve: CVE-2023-32042
cve: CVE-2023-32035
cve: CVE-2023-32034
cve: CVE-2023-32033
cve: CVE-2023-33173
cve: CVE-2023-33172
cve: CVE-2023-33167
cve: CVE-2023-33166
cve: CVE-2023-33164
cve: CVE-2023-33163
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5028240
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1718
dfn-cert: DFN-CERT-2023-1574
```

High (CVSS: 9.8)
NVT: Microsoft .NET XML Validation Security Feature Bypass Vulnerability (3141780)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-035

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v2.0.50727System.Security
↪.dll
File version:     2.0.50727.5420
Vulnerable range: 2.0.50727.5400 - 2.0.50727.5495
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to gain elevated privileges or disrupt the availability of applications that use the .NET framework.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft .NET Framework 3.0
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6 and 4.6.1
- Microsoft .NET Framework 3.5 and 3.5.1
- Microsoft .NET Framework 2.0 Service Pack 2

Vulnerability Insight

Flaw is due to improper handling of objects in memory by .NET's Windows Forms (WinForms) libraries and error when decrypting specially crafted XML data.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET XML Validation Security Feature Bypass Vulnerability (3141780)`

OID:1.3.6.1.4.1.25623.1.0.807311

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0132
url: https://support.microsoft.com/en-us/kb/3141780
url: https://technet.microsoft.com/library/security/MS16-035
cert-bund: CB-K16/0380
```

High (CVSS: 9.8)

NVT: Microsoft Windows Multiple Vulnerabilities (KB5025279)

Summary

This host is missing an important security update according to Microsoft KB5025279

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.26465
File checked:      C:\Windows\system32\Ntoskrnl.exe
File version:      6.1.7601.18741
```

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1.

Vulnerability Insight
Multiple flaws exist due to:
- An Elevation of Privilege Vulnerability in Windows Kernel.
- An Elevation of Privilege Vulnerability in Windows Ancillary Function Driver for WinSock.
- A Remote Code Execution Vulnerability in Microsoft Message Queuing.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5025279)`
OID:1.3.6.1.4.1.25623.1.0.832037
Version used: `2023-10-13T05:06:10Z`

References
```
cve: CVE-2023-21729
cve: CVE-2023-28308
cve: CVE-2023-28307
cve: CVE-2023-28306
cve: CVE-2023-28305
cve: CVE-2023-28302
cve: CVE-2023-28298
cve: CVE-2023-28293
cve: CVE-2023-28256
cve: CVE-2023-28278
cve: CVE-2023-28255
cve: CVE-2023-28253
cve: CVE-2023-28254
cve: CVE-2023-28276
cve: CVE-2023-28275
cve: CVE-2023-28252
cve: CVE-2023-28250
cve: CVE-2023-28272
cve: CVE-2023-28271
cve: CVE-2023-28268
cve: CVE-2023-28244
cve: CVE-2023-28266
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2023-28267
cve: CVE-2023-28241
cve: CVE-2023-28240
cve: CVE-2023-28238
cve: CVE-2023-28232
cve: CVE-2023-28231
cve: CVE-2023-28228
cve: CVE-2023-28229
cve: CVE-2023-28227
cve: CVE-2023-28223
cve: CVE-2023-28222
cve: CVE-2023-28220
cve: CVE-2023-28219
cve: CVE-2023-28218
cve: CVE-2023-28217
cve: CVE-2023-28216
cve: CVE-2023-24931
cve: CVE-2023-24912
cve: CVE-2023-21769
cve: CVE-2023-21727
cve: CVE-2023-21554
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5025279
cert-bund: WID-SEC-2023-0944
dfn-cert: DFN-CERT-2023-0808
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4486563)

Summary
This host is missing a critical security update according to Microsoft KB4486563

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24354
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code on a victim system, obtain information to further compromise the user's system, gain elevated privileges and conduct spoofing attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- Windows Jet Database Engine improperly handles objects in memory.
- Human Interface Devices (HID) component improperly handles objects in memory.
- Windows GDI component improperly discloses the contents of its memory.
- Internet Explorer improperly accesses objects in memory.
- Windows kernel improperly handles objects in memory.
- Win32k component fails to properly handle objects in memory.
- DHCP servers fails to properly handle network packets.
- Microsoft Server Message Block 2.0 (SMBv2) server improperly handles specially crafted requests.
- Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system.
- Microsoft browsers improperly handles specific redirects.
- Internet Explorer improperly handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4486563)`
OID:1.3.6.1.4.1.25623.1.0.814686
Version used: `2023-10-27T16:11:32Z`

References
```
cve: CVE-2019-0595
cve: CVE-2019-0596
cve: CVE-2019-0597
cve: CVE-2019-0598
cve: CVE-2019-0599
cve: CVE-2019-0600
cve: CVE-2019-0601
cve: CVE-2019-0602
cve: CVE-2019-0606
cve: CVE-2019-0615
cve: CVE-2019-0616
cve: CVE-2019-0618
cve: CVE-2019-0619
cve: CVE-2019-0621
cve: CVE-2019-0623
cve: CVE-2019-0625
cve: CVE-2019-0626
cve: CVE-2019-0628
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2019-0630
cve: CVE-2019-0635
cve: CVE-2019-0636
cve: CVE-2019-0654
cve: CVE-2019-0660
cve: CVE-2019-0661
cve: CVE-2019-0662
cve: CVE-2019-0664
cve: CVE-2019-0676
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4486563
cert-bund: CB-K19/0133
cert-bund: CB-K19/0132
cert-bund: CB-K19/0131
dfn-cert: DFN-CERT-2019-0319
dfn-cert: DFN-CERT-2019-0314
dfn-cert: DFN-CERT-2019-0311
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4467107)

Summary
This host is missing a critical security update according to Microsoft KB4467107.

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24291
File checked:      C:\Windows\system32\Advapi32.dll
File version:      6.1.7600.16385
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode which will empower them to install programs, view, change, delete data or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple flaws exist in Windows App Platform and Frameworks, Windows Graphics, Windows Wireless Networking, Windows Kernel, and Windows Server.
Please see the references for more details.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4467107)`
OID:1.3.6.1.4.1.25623.1.0.814173
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2018-8256
cve: CVE-2018-8407
cve: CVE-2018-8408
cve: CVE-2018-8415
cve: CVE-2018-8450
cve: CVE-2018-8471
cve: CVE-2018-8476
cve: CVE-2018-8544
cve: CVE-2018-8550
cve: CVE-2018-8552
cve: CVE-2018-8553
cve: CVE-2018-8562
cve: CVE-2018-8563
cve: CVE-2018-8565
cve: CVE-2018-8570
cve: CVE-2018-8589
cve: CVE-2018-1038
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4467107
cert-bund: CB-K18/1094
cert-bund: CB-K18/1090
cert-bund: CB-K18/0558
dfn-cert: DFN-CERT-2018-2340
dfn-cert: DFN-CERT-2018-2331
dfn-cert: DFN-CERT-2018-2330
dfn-cert: DFN-CERT-2018-0609
```

High (CVSS: 9.8)
NVT: Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows

Summary
Apache Log4j is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 1.2.15
Fixed version:     2.x
Installation
path / port:       C:\Program Files\Apache Software Foundation\tomcat\apache-tom
↪cat-8.0.33\webapps\axis2\WEB-INF\lib\log4j-1.2.15.jar
```

Solution:
Solution type: VendorFix
Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2.x which both addresses that vulnerability as well as numerous other issues in the previous versions.

Affected Software/OS
Apache Log4j versions 1.2.x through 1.2.17.

Vulnerability Insight
Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.117864
Version used: `2021-12-22T14:03:25Z`

References
```
cve: CVE-2019-17571
url: https://lists.apache.org/thread/173yrzw9trfy6xdydfz05tsvp79z8rt7
url: https://issues.apache.org/jira/browse/LOG4J2-1863
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-0138
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0770
cert-bund: WID-SEC-2022-0368
cert-bund: CB-K21/0493
cert-bund: CB-K20/0555
cert-bund: CB-K20/0363
dfn-cert: DFN-CERT-2023-0860
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-0988
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0050
```

High (CVSS: 9.8)
NVT: Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows

Summary

Apache Log4j is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.2.15
Fixed version:     2.x
Installation
path / port:       C:\ManageEngine\DesktopCentral_Server\lib\log4j-1.2.15.jar
```

Solution:

Solution type: VendorFix

Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2.x which both addresses that vulnerability as well as numerous other issues in the previous versions.

Affected Software/OS

Apache Log4j versions 1.2.x through 1.2.17.

Vulnerability Insight

Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.117864

Version used: `2021-12-22T14:03:25Z`

References

```
cve: CVE-2019-17571
url: https://lists.apache.org/thread/173yrzw9trfy6xdydfz05tsvp79z8rt7
url: https://issues.apache.org/jira/browse/LOG4J2-1863
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-0138
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0770
cert-bund: WID-SEC-2022-0368
cert-bund: CB-K21/0493
cert-bund: CB-K20/0555
cert-bund: CB-K20/0363
dfn-cert: DFN-CERT-2023-0860
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-0988
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0050
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4041681)

Summary
This host is missing a critical security update according to Microsoft KB4041681

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\win32k.sys
File version:     6.1.7601.17514
Vulnerable range:  Less than 6.1.7601.23914
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code, conduct denial-of-service, gain access to potentially sensitive information, take control of the affected system and gain escalated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- A spoofing vulnerability in the Windows implementation of wireless networking (KRACK)
- An error in the Microsoft Server Block Message (SMB) when an attacker sends specially crafted requests to the server.
- An error in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass.
- An error when the Windows kernel improperly handles objects in memory.
- An error when the Windows font library improperly handles specially crafted embedded fonts.
- An error when the Windows kernel-mode driver fails to properly handle objects in memory.
- An error when Internet Explorer improperly accesses objects in memory.
- An error in the Microsoft JET Database Engine that could allow remote code execution on an affected system.
- An error when Internet Explorer improperly handles objects in memory.
- An error when the Windows Graphics Component improperly handles objects in memory.
- An error in the way that the scripting engine handles objects in memory in Internet Explorer.
- An error when Internet Explorer improperly accesses objects in memory via the Microsoft Windows Text Services Framework.

. . . continues on next page . . .

... continued from previous page ...

- An error when Windows Search improperly handles objects in memory.
- An error in the way that Microsoft browsers access objects in memory.
- An error when the Windows kernel improperly initializes objects in memory.
- An error in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system.
- An error in the way that the Windows SMB Server handles certain requests.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4041681)`
OID:1.3.6.1.4.1.25623.1.0.812016
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-11762
cve: CVE-2017-8694
cve: CVE-2017-8717
cve: CVE-2017-8718
cve: CVE-2017-11763
cve: CVE-2017-11765
cve: CVE-2017-8727
cve: CVE-2017-11771
cve: CVE-2017-11772
cve: CVE-2017-11780
cve: CVE-2017-11781
cve: CVE-2017-11784
cve: CVE-2017-11785
cve: CVE-2017-11790
cve: CVE-2017-11793
cve: CVE-2017-11810
cve: CVE-2017-11813
cve: CVE-2017-11814
cve: CVE-2017-11815
cve: CVE-2017-11816
cve: CVE-2017-11817
cve: CVE-2017-11819
cve: CVE-2017-11822
cve: CVE-2017-11824
cve: CVE-2017-8689
cve: CVE-2017-13080
url: https://support.microsoft.com/en-us/help/4041681
url: http://www.securityfocus.com/bid/101108
url: http://www.securityfocus.com/bid/101100
url: http://www.securityfocus.com/bid/101161
url: http://www.securityfocus.com/bid/101162
url: http://www.securityfocus.com/bid/101109
url: http://www.securityfocus.com/bid/101111
```

... continues on next page ...

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/101142
url: http://www.securityfocus.com/bid/101114
url: http://www.securityfocus.com/bid/101116
url: http://www.securityfocus.com/bid/101110
url: http://www.securityfocus.com/bid/101140
url: http://www.securityfocus.com/bid/101147
url: http://www.securityfocus.com/bid/101149
url: http://www.securityfocus.com/bid/101077
url: http://www.securityfocus.com/bid/101141
url: http://www.securityfocus.com/bid/101081
url: http://www.securityfocus.com/bid/101083
url: http://www.securityfocus.com/bid/101093
url: http://www.securityfocus.com/bid/101136
url: http://www.securityfocus.com/bid/101094
url: http://www.securityfocus.com/bid/101095
url: http://www.securityfocus.com/bid/101121
url: http://www.securityfocus.com/bid/101122
url: http://www.securityfocus.com/bid/101099
url: http://www.securityfocus.com/bid/101128
url: http://www.securityfocus.com/bid/101274
cert-bund: WID-SEC-2022-2005
cert-bund: CB-K20/1098
cert-bund: CB-K18/0049
cert-bund: CB-K17/2224
cert-bund: CB-K17/2146
cert-bund: CB-K17/2144
cert-bund: CB-K17/2113
cert-bund: CB-K17/2081
cert-bund: CB-K17/2065
cert-bund: CB-K17/2049
cert-bund: CB-K17/1893
cert-bund: CB-K17/1892
cert-bund: CB-K17/1854
cert-bund: CB-K17/1851
cert-bund: CB-K17/1849
cert-bund: CB-K17/1840
cert-bund: CB-K17/1837
cert-bund: CB-K17/1832
cert-bund: CB-K17/1813
cert-bund: CB-K17/1812
cert-bund: CB-K17/1736
cert-bund: CB-K17/1707
cert-bund: CB-K17/1705
dfn-cert: DFN-CERT-2022-1201
dfn-cert: DFN-CERT-2020-2553
dfn-cert: DFN-CERT-2018-2314
dfn-cert: DFN-CERT-2018-1319
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1179
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2017-2325
dfn-cert: DFN-CERT-2017-2246
dfn-cert: DFN-CERT-2017-2241
dfn-cert: DFN-CERT-2017-2210
dfn-cert: DFN-CERT-2017-2176
dfn-cert: DFN-CERT-2017-2162
dfn-cert: DFN-CERT-2017-2139
dfn-cert: DFN-CERT-2017-1975
dfn-cert: DFN-CERT-2017-1972
dfn-cert: DFN-CERT-2017-1936
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1925
dfn-cert: DFN-CERT-2017-1922
dfn-cert: DFN-CERT-2017-1921
dfn-cert: DFN-CERT-2017-1917
dfn-cert: DFN-CERT-2017-1893
dfn-cert: DFN-CERT-2017-1892
dfn-cert: DFN-CERT-2017-1815
dfn-cert: DFN-CERT-2017-1783
dfn-cert: DFN-CERT-2017-1776
```

High (CVSS: 9.8)
NVT: Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check

Summary
Apache Log4j is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.2.17
Fixed version:     None
Installation
path / port:       C:\Program Files\elasticsearch-1.1.1\lib\log4j-1.2.17.jar
```

Solution:
Solution type: WillNotFix
No solution was made available by the vendor.
Note: Apache Log4j 1.x reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Affected Software/OS
Apache Log4j version 1.x.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The following vulnerabilities exist:
- CVE-2022-23302: Deserialization of untrusted data in JMSSink. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default.
- CVE-2022-23305: SQL injection in JDBC Appender. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default.
- CVE-2022-23307/CVE-2020-9493: A deserialization flaw in the Chainsaw component of Log4j 1.x can lead to malicious code execution.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check`
OID:1.3.6.1.4.1.25623.1.0.117902
Version used: `2023-10-18T05:05:17Z`

References

```
cve: CVE-2022-23302
cve: CVE-2022-23305
cve: CVE-2022-23307
cve: CVE-2020-9493
url: https://www.openwall.com/lists/oss-security/2022/01/18/3
url: https://www.openwall.com/lists/oss-security/2022/01/18/4
url: https://www.openwall.com/lists/oss-security/2022/01/18/5
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-1809
cert-bund: WID-SEC-2023-1027
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1909
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1780
cert-bund: WID-SEC-2022-1778
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1769
cert-bund: WID-SEC-2022-0754
cert-bund: WID-SEC-2022-0752
cert-bund: WID-SEC-2022-0738
cert-bund: WID-SEC-2022-0521
cert-bund: WID-SEC-2022-0169
cert-bund: CB-K22/0476
cert-bund: CB-K22/0471
cert-bund: CB-K22/0468
cert-bund: CB-K22/0464
cert-bund: CB-K22/0075
dfn-cert: DFN-CERT-2023-0860
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2311
dfn-cert: DFN-CERT-2022-2305
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1615
dfn-cert: DFN-CERT-2022-1472
dfn-cert: DFN-CERT-2022-1176
dfn-cert: DFN-CERT-2022-0874
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2022-0305
dfn-cert: DFN-CERT-2022-0292
dfn-cert: DFN-CERT-2022-0290
dfn-cert: DFN-CERT-2022-0204
dfn-cert: DFN-CERT-2022-0203
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4025341)

Summary
This host is missing a critical security update according to Microsoft KB4025341

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\clfs.sys
File version:     6.1.7600.16385
Vulnerable range:  Less than 6.1.7601.23841
```

Impact
Successful exploitation will allow an attacker to obtain information to further compromise the user's system, gain the same user rights as the current user, run arbitrary code in the context of another user, trick a user by redirecting the user to a specially crafted website, run processes in an elevated cretrieve the base address of the kernel driver from a compromised process, embed an ActiveX control marked 'safe for initialization' in an application or Microsoft Office document that hosts the Internet Explorer rendering engine, force the browser to send data that would otherwise be restricted to a destination web site of their choice, bypass Extended Protection for Authentication, read arbitrary files via an XML external entity (XXE) declaration and cause a denial of service.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple flaws exist when,
- Microsoft Windows fails to properly handle objects in memory.
- The way JavaScript engines render when handling objects in memory in Microsoft browsers.
- Windows Explorer improperly handles executable files and shares during rename operations.
- An affected Microsoft browser does not properly parse HTTP content.
- Windows improperly handles calls to Advanced Local Procedure Call (ALPC).
- Microsoft Windows when Kerberos falls back to NT LAN Manager (NTLM) Authentication Protocol as the default authentication protocol.
- Windows Kernel improperly handles objects in memory.
- The Windows kernel fails to properly initialize a memory address.
- PSObject wraps a CIM Instance.
- Microsoft Graphics Component fails to properly handle objects in memory.
- VBScript engine, when rendered in Internet Explorer, improperly handles objects in memory.
- Microsoft Browsers improperly handle redirect requests.
- Microsoft Windows when Kerberos fails to prevent tampering with the SNAME field during ticket exchange.
- Internet Explorer improperly accesses objects in memory.
- Windows System Information Console when it improperly parses XML input containing a reference to an external entity.
- Windows Performance Monitor Console when it improperly parses XML input containing a reference to an external entity.
- Microsoft WordPad parses specially crafted files.
- Windows Search improperly handles objects in memory.
- Windows Explorer attempts to open a non-existent file.
- Windows improperly handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4025341)`
OID:1.3.6.1.4.1.25623.1.0.811516
Version used: `2023-07-14T16:09:27Z`

References
```
cve: CVE-2017-8602
cve: CVE-2017-0170
cve: CVE-2017-8463
cve: CVE-2017-8467
cve: CVE-2017-8486
cve: CVE-2017-8495
cve: CVE-2017-8618
cve: CVE-2017-8556
cve: CVE-2017-8557
cve: CVE-2017-8563
cve: CVE-2017-8564
cve: CVE-2017-8565
cve: CVE-2017-8573
cve: CVE-2017-8577
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-8578
cve: CVE-2017-8580
cve: CVE-2017-8581
cve: CVE-2017-8582
cve: CVE-2017-8587
cve: CVE-2017-8588
cve: CVE-2017-8589
cve: CVE-2017-8590
cve: CVE-2017-8592
url: https://support.microsoft.com/en-us/help/4025341
url: http://www.securityfocus.com/bid/99390
url: http://www.securityfocus.com/bid/99389
url: http://www.securityfocus.com/bid/99409
url: http://www.securityfocus.com/bid/99414
url: http://www.securityfocus.com/bid/99424
url: http://www.securityfocus.com/bid/99399
url: http://www.securityfocus.com/bid/99439
url: http://www.securityfocus.com/bid/99398
url: http://www.securityfocus.com/bid/99402
url: http://www.securityfocus.com/bid/99428
url: http://www.securityfocus.com/bid/99394
url: http://www.securityfocus.com/bid/99431
url: http://www.securityfocus.com/bid/99416
url: http://www.securityfocus.com/bid/99419
url: http://www.securityfocus.com/bid/99421
url: http://www.securityfocus.com/bid/99423
url: http://www.securityfocus.com/bid/99429
url: http://www.securityfocus.com/bid/99413
url: http://www.securityfocus.com/bid/99400
url: http://www.securityfocus.com/bid/99425
url: http://www.securityfocus.com/bid/99427
url: http://www.securityfocus.com/bid/99396
cert-bund: CB-K17/1168
cert-bund: CB-K17/1161
cert-bund: CB-K17/1160
dfn-cert: DFN-CERT-2017-1202
dfn-cert: DFN-CERT-2017-1198
dfn-cert: DFN-CERT-2017-1197
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4025337)

Summary

This host is missing a critical security update according to Microsoft KB4025337

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
File checked:     C:\Windows\system32\win32k.sys
File version:     6.1.7601.17514
Vulnerable range:  Less than 6.1.7601.23848
```

Impact

Successful exploitation will allow an attacker to force the browser to send data that would otherwise be restricted to a destination web site of their choice, to obtain information to further compromise the user's system, to run arbitrary code in kernel mode, to run processes in an elevated context, to run arbitrary code in the context of another user, to could read arbitrary files via an XML external entity (XXE) declaration, to bypass Extended Protection for Authentication, take control of the affected system, retrieve the base address of the kernel driver from a compromised process, execute malicious code on a vulnerable system, cause a denial of service, obtain information to further compromise the system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist:

- When Microsoft Browsers improperly handle redirect requests.
- In Microsoft Windows when Win32k fails to properly handle objects in memory.
- In Windows when the Microsoft Graphics Component fails to properly handle objects in memory.
- In Microsoft Windows when Kerberos falls back to NT LAN Manager (NTLM) Authentication Protocol as the default authentication protocol.
- When Windows Explorer improperly handles executable files and shares during rename operations.
- When Windows improperly handles objects in memory.
- In the Windows System Information Console when it improperly parses XML input containing a reference to an external entity.
- In Microsoft Windows when Kerberos fails to prevent tampering with the SNAME field during ticket exchange.
- In the way that Microsoft WordPad parses specially crafted files.
- When Windows Search handles objects in memory.
- When the Windows kernel fails to properly initialize a memory address, allowing an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass.
- In PowerShell when PSObject wraps a CIM Instance.
- When Windows Explorer attempts to open a non-existent file.
- In the Windows Performance Monitor Console when it improperly parses XML input containing a reference to an external entity.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4025337)`

OID:1.3.6.1.4.1.25623.1.0.811519

Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0170
cve: CVE-2017-8463
cve: CVE-2017-8467
cve: CVE-2017-8486
cve: CVE-2017-8495
cve: CVE-2017-8556
cve: CVE-2017-8557
cve: CVE-2017-8563
cve: CVE-2017-8564
cve: CVE-2017-8565
cve: CVE-2017-8573
cve: CVE-2017-8577
cve: CVE-2017-8578
cve: CVE-2017-8580
cve: CVE-2017-8581
cve: CVE-2017-8582
cve: CVE-2017-8587
cve: CVE-2017-8588
cve: CVE-2017-8589
cve: CVE-2017-8590
cve: CVE-2017-8592
url: https://support.microsoft.com/en-us/help/4025337
url: http://www.securityfocus.com/bid/99389
url: http://www.securityfocus.com/bid/99409
url: http://www.securityfocus.com/bid/99414
url: http://www.securityfocus.com/bid/99424
url: http://www.securityfocus.com/bid/99439
url: http://www.securityfocus.com/bid/99398
url: http://www.securityfocus.com/bid/99402
url: http://www.securityfocus.com/bid/99428
url: http://www.securityfocus.com/bid/99394
url: http://www.securityfocus.com/bid/99431
url: http://www.securityfocus.com/bid/99416
url: http://www.securityfocus.com/bid/99419
url: http://www.securityfocus.com/bid/99421
url: http://www.securityfocus.com/bid/99423
url: http://www.securityfocus.com/bid/99429
url: http://www.securityfocus.com/bid/99413
url: http://www.securityfocus.com/bid/99400
```

... continues on next page ...

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/99425
url: http://www.securityfocus.com/bid/99427
url: http://www.securityfocus.com/bid/99396
cert-bund: CB-K17/1168
cert-bund: CB-K17/1161
cert-bund: CB-K17/1160
dfn-cert: DFN-CERT-2017-1202
dfn-cert: DFN-CERT-2017-1198
dfn-cert: DFN-CERT-2017-1197
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4022722)

Summary
This host is missing a critical security update according to Microsoft KB4022722

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Gdi32.dll
File version:     6.1.7601.17514
Vulnerable range:  Less than 6.1.7601.23807
```

Impact
Successful exploitation will allow attackers to gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs. View, change, or delete data, or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1

Vulnerability Insight
This security update includes quality improvements.
- Addressed issue where, after installing KB3164035, users cannot print enhanced metafiles (EMF) or documents containing bitmaps rendered out of bounds using the BitMapSection(DIBSection) function.
- Addressed issue where updates were not correctly installing all components and would prevent them from booting.
- Addressed issue where an unsupported hardware notification is shown and Windows Updates not scanning, for systems using the AMD Carrizo DDR4 processor. For the affected systems, follow the steps in the Additional Information section to install this update.

. . . continues on next page . . .

. . . continued from previous page . . .

- Security updates to Windows kernel, Microsoft Graphics Component, Microsoft Uniscribe, Windows kernel-mode drivers, the Windows OS, Windows COM and Windows shell.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4022722)`
OID:1.3.6.1.4.1.25623.1.0.811168
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0193
cve: CVE-2017-8472
cve: CVE-2017-8473
cve: CVE-2017-8475
cve: CVE-2017-8527
cve: CVE-2017-8528
cve: CVE-2017-0260
cve: CVE-2017-0282
cve: CVE-2017-8476
cve: CVE-2017-8477
cve: CVE-2017-8531
cve: CVE-2017-0283
cve: CVE-2017-0284
cve: CVE-2017-8478
cve: CVE-2017-8479
cve: CVE-2017-8532
cve: CVE-2017-8533
cve: CVE-2017-0285
cve: CVE-2017-0286
cve: CVE-2017-0287
cve: CVE-2017-8480
cve: CVE-2017-8481
cve: CVE-2017-8534
cve: CVE-2017-8543
cve: CVE-2017-8544
cve: CVE-2017-0288
cve: CVE-2017-0289
cve: CVE-2017-8482
cve: CVE-2017-8483
cve: CVE-2017-8484
cve: CVE-2017-8485
cve: CVE-2017-8553
cve: CVE-2017-0294
cve: CVE-2017-0296
cve: CVE-2017-8488
cve: CVE-2017-8489
cve: CVE-2017-8490
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-0297
cve: CVE-2017-0298
cve: CVE-2017-0299
cve: CVE-2017-8491
cve: CVE-2017-8492
cve: CVE-2017-0300
cve: CVE-2017-8462
cve: CVE-2017-8464
cve: CVE-2017-8469
cve: CVE-2017-8470
cve: CVE-2017-8471
cve: CVE-2017-8554
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4022722
url: http://www.securityfocus.com/bid/98878
url: http://www.securityfocus.com/bid/98851
url: http://www.securityfocus.com/bid/98852
url: http://www.securityfocus.com/bid/98853
url: http://www.securityfocus.com/bid/98933
url: http://www.securityfocus.com/bid/98949
url: http://www.securityfocus.com/bid/98810
url: http://www.securityfocus.com/bid/98885
url: http://www.securityfocus.com/bid/98903
url: http://www.securityfocus.com/bid/98854
url: http://www.securityfocus.com/bid/98819
url: http://www.securityfocus.com/bid/98920
url: http://www.securityfocus.com/bid/98918
url: http://www.securityfocus.com/bid/98845
url: http://www.securityfocus.com/bid/98856
url: http://www.securityfocus.com/bid/98820
url: http://www.securityfocus.com/bid/98821
url: http://www.securityfocus.com/bid/98914
url: http://www.securityfocus.com/bid/98891
url: http://www.securityfocus.com/bid/98922
url: http://www.securityfocus.com/bid/98857
url: http://www.securityfocus.com/bid/98862
url: http://www.securityfocus.com/bid/98822
url: http://www.securityfocus.com/bid/98824
url: http://www.securityfocus.com/bid/98826
url: http://www.securityfocus.com/bid/98923
url: http://www.securityfocus.com/bid/98929
url: http://www.securityfocus.com/bid/98858
url: http://www.securityfocus.com/bid/98859
url: http://www.securityfocus.com/bid/98847
url: http://www.securityfocus.com/bid/98860
url: http://www.securityfocus.com/bid/98940
```

. . . continues on next page . . .

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/98837
url: http://www.securityfocus.com/bid/98839
url: http://www.securityfocus.com/bid/98864
url: http://www.securityfocus.com/bid/98865
url: http://www.securityfocus.com/bid/98867
url: http://www.securityfocus.com/bid/98840
url: http://www.securityfocus.com/bid/98884
url: http://www.securityfocus.com/bid/98869
url: http://www.securityfocus.com/bid/98870
url: http://www.securityfocus.com/bid/98901
url: http://www.securityfocus.com/bid/98900
url: http://www.securityfocus.com/bid/98818
url: http://www.securityfocus.com/bid/98842
url: http://www.securityfocus.com/bid/98848
url: http://www.securityfocus.com/bid/98849
cert-bund: CB-K17/1168
cert-bund: CB-K17/0993
cert-bund: CB-K17/0992
cert-bund: CB-K17/0989
dfn-cert: DFN-CERT-2017-1202
dfn-cert: DFN-CERT-2017-1026
dfn-cert: DFN-CERT-2017-1023
dfn-cert: DFN-CERT-2017-1022
```

High (CVSS: 9.8)
NVT: Microsoft Windows Multiple Vulnerabilities (3192884)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-120.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23545
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode, also could take control of the affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2

... continues on next page ...

. . . continued from previous page . . .

- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight

Multiple flaws exist due to
- The way that the Windows Graphics Device Interface (GDI) handles objects in memory.
- The Windows kernel fails to properly handle objects in memory.
- The Windows font library improperly handles specially crafted embedded fonts.
- The Windows Graphics Component improperly handles objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (3192884)`
OID:1.3.6.1.4.1.25623.1.0.809346
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2016-3209
cve: CVE-2016-3262
cve: CVE-2016-3263
cve: CVE-2016-3270
cve: CVE-2016-3393
cve: CVE-2016-3396
cve: CVE-2016-7182
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3192884
url: http://www.securityfocus.com/bid/93385
url: http://www.securityfocus.com/bid/93390
url: http://www.securityfocus.com/bid/93394
url: http://www.securityfocus.com/bid/93403
url: http://www.securityfocus.com/bid/93377
url: http://www.securityfocus.com/bid/93380
url: http://www.securityfocus.com/bid/93395
url: https://technet.microsoft.com/en-us/library/security/MS16-120
url: https://technet.microsoft.com/library/security/MS16-120
cert-bund: CB-K16/1582
cert-bund: CB-K16/1578
cert-bund: CB-K16/1576
cert-bund: CB-K16/1575
```

High (CVSS: 9.8)
NVT: Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check

Summary
Apache Log4j is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.2.17
Fixed version:     None
Installation
path / port:       C:\Program Files\Apache Software Foundation\tomcat\apache-tom
↪cat-8.0.33\webapps\struts2-rest-showcase\WEB-INF\lib\log4j-1.2.17.jar
```

Solution:
Solution type: WillNotFix
No solution was made available by the vendor.
Note: Apache Log4j 1.x reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Affected Software/OS
Apache Log4j version 1.x.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-23302: Deserialization of untrusted data in JMSSink. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default.
- CVE-2022-23305: SQL injection in JDBC Appender. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default.
- CVE-2022-23307/CVE-2020-9493: A deserialization flaw in the Chainsaw component of Log4j 1.x can lead to malicious code execution.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check`
OID:1.3.6.1.4.1.25623.1.0.117902
Version used: `2023-10-18T05:05:17Z`

References

```
cve: CVE-2022-23302
cve: CVE-2022-23305
cve: CVE-2022-23307
cve: CVE-2020-9493
url: https://www.openwall.com/lists/oss-security/2022/01/18/3
url: https://www.openwall.com/lists/oss-security/2022/01/18/4
url: https://www.openwall.com/lists/oss-security/2022/01/18/5
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1809
cert-bund: WID-SEC-2023-1027
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1909
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1780
cert-bund: WID-SEC-2022-1778
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1769
cert-bund: WID-SEC-2022-0754
cert-bund: WID-SEC-2022-0752
cert-bund: WID-SEC-2022-0738
cert-bund: WID-SEC-2022-0521
cert-bund: WID-SEC-2022-0169
cert-bund: CB-K22/0476
cert-bund: CB-K22/0471
cert-bund: CB-K22/0468
cert-bund: CB-K22/0464
cert-bund: CB-K22/0075
dfn-cert: DFN-CERT-2023-0860
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2311
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-1615
dfn-cert: DFN-CERT-2022-1472
dfn-cert: DFN-CERT-2022-1176
dfn-cert: DFN-CERT-2022-0874
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2022-0305
dfn-cert: DFN-CERT-2022-0292
dfn-cert: DFN-CERT-2022-0290
dfn-cert: DFN-CERT-2022-0204
dfn-cert: DFN-CERT-2022-0203
```

High (CVSS: 9.4)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5003667)

Summary
This host is missing a critical security update according to Microsoft KB5003667

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.25631
File checked:      C:\Windows\system32\advapi32.dll
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
File version:      6.1.7600.16385
```

Impact

Successful exploitation will allow an attacker to perform remote code execution, gain access to potentially sensitive data, conduct spoofing and elevate privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- An elevation of privilege vulnerability in Windows Common Log File System Driver.
- A security feature bypass vulnerability in Kerberos AppContainer.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5003667)`

OID:1.3.6.1.4.1.25623.1.0.818137

Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2021-1675
cve: CVE-2021-26414
cve: CVE-2021-31199
cve: CVE-2021-31201
cve: CVE-2021-31953
cve: CVE-2021-31954
cve: CVE-2021-31956
cve: CVE-2021-31958
cve: CVE-2021-31959
cve: CVE-2021-31962
cve: CVE-2021-31968
cve: CVE-2021-31971
cve: CVE-2021-31973
cve: CVE-2021-33742
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5003667
cert-bund: CB-K21/0633
```

. . . continues on next page . . .

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2021-1232

High (CVSS: 9.3)
NVT: Microsoft IE Developer Tools WMITools and Windows Messenger ActiveX Control Vulnerability (2508272)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS11-027.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.
As a workaround set the killbit for the following CLSIDs:
}1a6fe369-f28c-4ad9-a3e6-2bcb50807cf1}, }2745E5F5-D234-11D0-847A-00C04FD7BB08}, }FB7199AB-79BF-11d2-8D94-0000F875C541}

Affected Software/OS
- Microsoft Windows 7 Service Pack 1 and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows 2K3 Service Pack 2 and prior
- Microsoft Windows Vista Service Pack 1/2 and prior
- Microsoft Windows Server 2008 Service Pack 1/2 and prior

Vulnerability Insight
An unspecified error exists in the IE Developer Tools(iedvtool.dll), WMITools (WBEMSingleView.OCX) and Windows Messenger (msgsc.dll) ActiveX Controls when used with Internet Explorer. Attackers can execute arbitrary code by tricking a user into visiting a specially crafted web page.

Vulnerability Detection Method
Details: `Microsoft IE Developer Tools WMITools and Windows Messenger ActiveX Control Vul.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.900281
Version used: `2022-04-28T13:38:57Z`

References
cve: CVE-2010-0811
cve: CVE-2010-3973
cve: CVE-2011-1243

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2010-4588
url: http://www.exploit-db.com/exploits/15809/
url: http://www.securityfocus.com/bid/40490
url: http://www.securityfocus.com/bid/45546
url: http://www.securityfocus.com/bid/47197
url: http://xforce.iss.net/xforce/xfdb/64250
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms
↪11-027
url: http://support.microsoft.com/kb/240797
dfn-cert: DFN-CERT-2010-0742
```

High (CVSS: 9.3)
NVT: Microsoft Security Update For Microsoft Office, .NET Framework, and Silverlight (2681578)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-034.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow an attacker to gain escalated privileges and execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 4
- Microsoft Silverlight 4 and 5
- Microsoft .NET Framework 3.5.1
- Microsoft Office 2003 Service Pack 3
- Microsoft Office 2007 Service Pack 2
- Microsoft Office 2010 Service Pack 1
- Microsoft .NET Framework 3.0 Service Pack 2
- Microsoft Windows 7 Service Pack 1 and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows 2003 Service Pack 2 and prior
- Microsoft Windows Vista Service Pack 2 and prior
- Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to

. . . continues on next page . . .

. . . continued from previous page . . .

- An error exists when parsing TrueType fonts.
- An error in the t2embed.dll module when parsing TrueType fonts can be exploited via a specially crafted TTF file.
- An error in GDI+ when handling certain records can be exploited via a specially crafted EMF image file.
- An error in win32k.sys related to certain Windows and Messages handling can be exploited to execute arbitrary code in the context of another process.
- An error in win32k.sys when handling keyboard layout files can be exploited to execute arbitrary code in the context of another process.
- An error in win32k.sys related to scrollbar calculations can be exploited to execute arbitrary code in the context of another process.

Vulnerability Detection Method

Details: `Microsoft Security Update For Microsoft Office, .NET Framework, and Silverlight.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902832
Version used: `2024-06-21T05:05:42Z`

References

```
cve: CVE-2011-3402
cve: CVE-2012-0159
cve: CVE-2012-0162
cve: CVE-2012-0164
cve: CVE-2012-0165
cve: CVE-2012-0167
cve: CVE-2012-0176
cve: CVE-2012-0180
cve: CVE-2012-0181
cve: CVE-2012-1848
url: http://support.microsoft.com/kb/2681578
url: http://www.securityfocus.com/bid/50462
url: http://www.securityfocus.com/bid/53324
url: http://www.securityfocus.com/bid/53326
url: http://www.securityfocus.com/bid/53327
url: http://www.securityfocus.com/bid/53335
url: http://www.securityfocus.com/bid/53347
url: http://www.securityfocus.com/bid/53351
url: http://www.securityfocus.com/bid/53358
url: http://www.securityfocus.com/bid/53360
url: http://www.securityfocus.com/bid/53363
url: http://www.securitytracker.com/id/1027048
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-034
dfn-cert: DFN-CERT-2012-1128
dfn-cert: DFN-CERT-2012-0901
```

High (CVSS: 9.3)
NVT: Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (2685939)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-036.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to execute arbitrary code as the logged-on user or cause a denial of service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
The way that the Remote Desktop Protocol accesses an object in memory that has been improperly initialized or has been deleted or the way RDP service processes the packets, allows to run arbitrary code on the target system.

Vulnerability Detection Method
Details: `Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (2685939)`
OID:1.3.6.1.4.1.25623.1.0.902683
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2012-0173
url: http://support.microsoft.com/kb/2685939
url: http://www.securityfocus.com/bid/53826
url: http://www.securitytracker.com/id/1027148
url: http://www.securelist.com/en/advisories/49384
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-036
dfn-cert: DFN-CERT-2012-1118
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Remote Code Execution Vulnerability (2745030)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-074.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code with the privileges of the currently logged-in user. Failed attacks will cause denial-of-service conditions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0, 3.5, 3.5.1, and 4.

Vulnerability Insight
- An error within permissions checking of objects that perform reflection can be exploited via a specially crafted XAML Browser Application (XBAP) or an untrusted .NET application.
- An sanitisation error when processing partially trusted code can be exploited to disclose certain data via a specially crafted XAML Browser Application (XBAP) or an untrusted .NET application.
- The Entity Framework component loads certain libraries in an insecure manner, which can be exploited to load arbitrary libraries by tricking a user into opening certain files located on a remote WebDAV or SMB share.
- A validation error when acquiring proxy settings via the Web Proxy Auto-Discovery (WPAD) can be exploited to execute JavaScript code with reduced restrictions.
- An error within permissions checking of Windows Presentation Foundation (WPF) objects that perform reflection can be exploited via a specially crafted XAML Browser Application (XBAP) or an untrusted .NET application.

Vulnerability Detection Method
Details: `Microsoft .NET Framework Remote Code Execution Vulnerability (2745030)`
OID:1.3.6.1.4.1.25623.1.0.902934
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2012-1895
cve: CVE-2012-1896
cve: CVE-2012-2519
cve: CVE-2012-4776
cve: CVE-2012-4777
url: http://support.microsoft.com/kb/2745030
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/56455
url: http://www.securityfocus.com/bid/56456
url: http://www.securityfocus.com/bid/56462
url: http://www.securityfocus.com/bid/56464
url: http://support.microsoft.com/kb/2729456
url: http://support.microsoft.com/kb/2729460
url: http://support.microsoft.com/kb/2729449
url: http://support.microsoft.com/kb/2729452
url: http://support.microsoft.com/kb/2729451
url: http://support.microsoft.com/kb/2729450
url: http://support.microsoft.com/kb/2729453
url: http://support.microsoft.com/kb/2698023
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-074
dfn-cert: DFN-CERT-2012-2111
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Remote Code Execution Vulnerability (2706726)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-038.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow an attacker to execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 4
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 2.0 Service Pack 2

Vulnerability Insight
The flaw is due to an error within the framework when handling pointers and can be exploited to corrupt memory via a specially crafted web page.

Vulnerability Detection Method
Details: `Microsoft .NET Framework Remote Code Execution Vulnerability (2706726)`
OID:1.3.6.1.4.1.25623.1.0.902841
Version used: `2022-05-25T07:40:23Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2012-1855
url: http://support.microsoft.com/kb/2706726
url: http://www.securityfocus.com/bid/53861
url: http://www.securitytracker.com/id/1027149
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-038
dfn-cert: DFN-CERT-2012-1117
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Remote Code Execution Vulnerability (2693777)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS12-035.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow an attacker to execute arbitrary code with the privileges of the currently logged-in user. Failed attacks will cause denial-of-service conditions.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5 SP1, 3.5.1, and 4.

Vulnerability Insight

The flaws are due to

- An error within the .NET Framework does not properly serialize user input and can be exploited to treat untrusted input as trusted.
- An error within the .NET Framework does not properly handle exceptions when serializing objects and can be exploited via partially trusted assemblies.

Vulnerability Detection Method

Details: `Microsoft .NET Framework Remote Code Execution Vulnerability (2693777)`
OID:1.3.6.1.4.1.25623.1.0.902833
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-0160
cve: CVE-2012-0161
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://support.microsoft.com/kb/2693777
url: http://www.securityfocus.com/bid/53356
url: http://www.securityfocus.com/bid/53357
url: http://www.securitytracker.com/id/1027036
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-035
cert-bund: CB-K19/1121
dfn-cert: DFN-CERT-2012-0902
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Remote Code Execution Vulnerabilities (2878890)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS13-082.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to execute the arbitrary code, exhaust available system resource, cause a DoS (Denial of Service) and compromise the system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 2.x
- Microsoft .NET Framework 3.x
- Microsoft .NET Framework 4.x

Vulnerability Insight
Multiple flaws are due to:
- An unspecified error when handling OpenType fonts (OTF).
- An error when when expanding entity references.
- An unspecified error when parsing JSON data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Remote Code Execution Vulnerabilities (2878890)`
OID:1.3.6.1.4.1.25623.1.0.903412
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-3128
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-3860
cve: CVE-2013-3861
url: http://support.microsoft.com/kb/2878890
url: http://www.securityfocus.com/bid/62807
url: http://www.securityfocus.com/bid/62819
url: http://www.securityfocus.com/bid/62820
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-082
cert-bund: CB-K13/0762
cert-bund: CB-K13/0760
dfn-cert: DFN-CERT-2013-1755
dfn-cert: DFN-CERT-2013-1753
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Privilege Elevation Vulnerability (3057134)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-048.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to gain elevated privileges or disrupt the availability of applications that use the .NET framework.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 1.1 Service Pack 1
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5, 4.5.1, and 4.5.2

Vulnerability Insight
Flaw is due to improper handling of objects in memory by .NET's Windows Forms (WinForms) libraries and error when decrypting specially crafted XML data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Privilege Elevation Vulnerability (3057134)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.805178
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1672
cve: CVE-2015-1673
url: https://support.microsoft.com/en-us/kb/3057134
url: http://www.securityfocus.com/bid/74482
url: http://www.securityfocus.com/bid/74487
url: https://technet.microsoft.com/library/security/MS15-048
cert-bund: CB-K15/0668
dfn-cert: DFN-CERT-2015-0689
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Privilege Elevation Vulnerability (3005210)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-072.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to bypass certain security restrictions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 1.1, 2.0, 3.5, 3.5.1, 4.0, 4.5, 4.5.1 and 4.5.2.

Vulnerability Insight
A flaw exists due to the way .NET Framework handles TypeFilterLevel checks for some malformed objects.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Privilege Elevation Vulnerability (3005210)`
OID:1.3.6.1.4.1.25623.1.0.804791
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2014-4149
url: https://support.microsoft.com/kb/3005210
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/70979
url: https://technet.microsoft.com/library/security/MS14-072
cert-bund: CB-K14/1402
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3038314)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-032.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x and VBScript 5.8 on IE 8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to improper handling memory objects when accessing it and some user-supplied input is not properly validated.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3038314)`
OID:1.3.6.1.4.1.25623.1.0.805163
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-1652
cve: CVE-2015-1657
cve: CVE-2015-1659
cve: CVE-2015-1660
cve: CVE-2015-1661
cve: CVE-2015-1662
cve: CVE-2015-1665
cve: CVE-2015-1666
cve: CVE-2015-1667
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-1668
url: https://support.microsoft.com/en-us/kb/3038314
url: https://technet.microsoft.com/library/security/MS15-032
cert-bund: CB-K15/0521
dfn-cert: DFN-CERT-2015-0540
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Privilege Elevation Vulnerabilities (3089662)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-101.

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v2.0.50727System.Componen
↪tModel.DataAnnotations.dll
File version:     0
Vulnerable range: Less than 2.0.50727.5492
```

Impact
Successful exploitation will allow an attacker to conduct denial-of-service attack and take complete control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5, 4.5.1, and 4.5.2
- Microsoft .NET Framework 4.6 and 4.6 RC

Vulnerability Insight
Multiple flaws exist due to:
- An unspecified error in the way that the .NET Framework validates the number of objects in memory before copying those objects into an array.
- Application fails to properly handle certain specially crafted requests.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Privilege Elevation Vulnerabilities (3089662)`
OID:1.3.6.1.4.1.25623.1.0.805978
Version used: `2023-07-25T05:05:58Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2015-2504
cve: CVE-2015-2526
url: https://support.microsoft.com/en-us/kb/3089662
url: https://technet.microsoft.com/library/security/ms15-101
cert-bund: CB-K15/1321
dfn-cert: DFN-CERT-2015-1385
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Privilege Elevation Vulnerabilities (3089662)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-101.

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v2.0.50727System.Drawing.
↪dll
File version:     2.0.50727.5420
Vulnerable range: Less than 2.0.50727.5492
```

Impact

Successful exploitation will allow an attacker to conduct denial-of-service attack and take complete control of an affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5, 4.5.1, and 4.5.2
- Microsoft .NET Framework 4.6 and 4.6 RC

Vulnerability Insight

Multiple flaws exist due to:

- An unspecified error in the way that the .NET Framework validates the number of objects in memory before copying those objects into an array.
- Application fails to properly handle certain specially crafted requests.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

... continued from previous page ...

Details: `Microsoft .NET Framework Privilege Elevation Vulnerabilities (3089662)`
OID:1.3.6.1.4.1.25623.1.0.805978
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2504
cve: CVE-2015-2526
url: https://support.microsoft.com/en-us/kb/3089662
url: https://technet.microsoft.com/library/security/ms15-101
cert-bund: CB-K15/1321
dfn-cert: DFN-CERT-2015-1385
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Privilege Elevation Vulnerability (2769324)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-004.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code with the privileges of the currently logged-in user. Failed attacks will cause denial-of-service conditions.

Solution:

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0, 3.5, 3.5.1, 4 and 4.5.

Vulnerability Insight

- An error within the System Drawing namespace of Windows Forms when handling pointers can be exploited to bypass CAS (Code Access Security) restrictions and disclose information.
- An error within WinForms when handling certain objects can be exploited to cause a buffer overflow.
- A boundary error within the System.DirectoryServices.Protocols namespace when handling objects can be exploited to cause a buffer overflow.
- A double construction error within the framework does not validate object permissions and can be exploited via a specially crafted XAML Browser Application (XBAP) or an untrusted .NET application.

Vulnerability Detection Method

Details: `Microsoft .NET Framework Privilege Elevation Vulnerability (2769324)`

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.902939
Version used: 2022-05-25T07:40:23Z

References

```
cve: CVE-2013-0001
cve: CVE-2013-0002
cve: CVE-2013-0003
cve: CVE-2013-0004
url: http://support.microsoft.com/kb/2769324
url: http://www.securityfocus.com/bid/57113
url: http://www.securityfocus.com/bid/57114
url: http://www.securityfocus.com/bid/57124
url: http://www.securityfocus.com/bid/57126
url: http://support.microsoft.com/kb/2742613
url: http://support.microsoft.com/kb/2742595
url: http://support.microsoft.com/kb/2756921
url: http://support.microsoft.com/kb/2756920
url: http://support.microsoft.com/kb/2742599
url: http://support.microsoft.com/kb/2742598
url: http://support.microsoft.com/kb/2756919
url: http://support.microsoft.com/kb/2756918
url: http://support.microsoft.com/kb/2742601
url: http://support.microsoft.com/kb/2742596
url: http://support.microsoft.com/kb/2742597
url: http://support.microsoft.com/kb/2742604
url: http://support.microsoft.com/kb/2742607
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-004
cert-bund: CB-K19/1121
dfn-cert: DFN-CERT-2013-0056
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Multiple Vulnerabilities (2861561)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-052.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow an attacker to execute arbitrary code, bypass security mechanism and take complete control of an affected system.

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 1.0, 1.1, 2.0, 3.0, 3.5, 3.5.1, 4.0 and 4.5.

Vulnerability Insight
Multiple flaws due to:
- Improper handling of TrueType font and multidimensional arrays of small structures
- Improper validation of permissions for certain objects performing reflection and delegate objects during serialization

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Multiple Vulnerabilities (2861561)`
OID:1.3.6.1.4.1.25623.1.0.902985
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2013-3129
cve: CVE-2013-3131
cve: CVE-2013-3132
cve: CVE-2013-3133
cve: CVE-2013-3134
cve: CVE-2013-3171
url: http://support.microsoft.com/kb/2861561
url: http://www.securityfocus.com/bid/60932
url: http://www.securityfocus.com/bid/60933
url: http://www.securityfocus.com/bid/60934
url: http://www.securityfocus.com/bid/60935
url: http://www.securityfocus.com/bid/60937
url: http://www.securityfocus.com/bid/60978
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-052
dfn-cert: DFN-CERT-2013-1267
dfn-cert: DFN-CERT-2013-1264
dfn-cert: DFN-CERT-2013-1262
```

High (CVSS: 9.3)
NVT: Microsoft JScript and VBScript Engines Remote Code Execution Vulnerability (2706045)

Summary
This host is missing an important security update according to Microsoft Bulletin MS12-056.

Vulnerability Detection Result
```
Vulnerable range:  < 5.8.7600.17045, 5.8.7600.20000 - 5.8.7600.21237, 5.8.7601.1
```

. . . continues on next page . . .

... continued from previous page ...

```
↪7000 - 5.8.7601.17865, 5.8.7601.21000 - 5.8.7601.22023
File checked:      C:\WindowsSystem32\Vbscript.dll
File version:      5.8.7601.17514
```

Impact
Successful exploitation could allow remote attackers to execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x64 Edition Service Pack 1 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 2003 x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
The flaw is caused by an integer overflow error in the JScript and VBScript scripting engines when calculating the size of an object in memory.

Vulnerability Detection Method
Details: `Microsoft JScript and VBScript Engines Remote Code Execution Vulnerability (270.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903037
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2012-2523
url: http://support.microsoft.com/kb/2706045
url: http://www.securityfocus.com/bid/54945
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-056
dfn-cert: DFN-CERT-2012-1575
dfn-cert: DFN-CERT-2012-1573
```

High (CVSS: 9.3)
NVT: Microsoft Windows File Handling Component Remote Code Execution Vulnerability (2758857)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-081.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow attacker to gain the same user rights as the current user by execute arbitrary code with system-level privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

The flaw is due to error in the File Handling component, which allow user browses to a folder that contains a file or sub folder names and can be exploited to corrupt memory via a file with a specially crafted filename.

Vulnerability Detection Method

Details: `Microsoft Windows File Handling Component Remote Code Execution Vulnerability (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.901304

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-4774
url: http://support.microsoft.com/kb/2758857
url: http://www.securityfocus.com/bid/56443
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-081
dfn-cert: DFN-CERT-2012-2233
```

High (CVSS: 9.3)

NVT: Microsoft Internet Explorer RCE vulnerability (3088903)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-093.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: 8.0.7601.17000 - 8.0.7601.18967
```

Impact

Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight

The error exists due to multiple improper handling of memory objects.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Internet Explorer RCE vulnerability (3088903)`

OID:1.3.6.1.4.1.25623.1.0.805959

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2502
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/3088903
url: http://www.securityfocus.com/bid/76403
url: https://support.microsoft.com/kb/3087985
url: https://technet.microsoft.com/en-us/library/security/MS15-093
cert-bund: CB-K15/1215
dfn-cert: DFN-CERT-2015-1283
```

High (CVSS: 9.3)

NVT: Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3058515)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-056.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to improper handling memory objects when accessing it and does not properly validate permissions under specific conditions.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3058515)`
OID:1.3.6.1.4.1.25623.1.0.805196
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-1687
cve: CVE-2015-1730
cve: CVE-2015-1731
cve: CVE-2015-1732
cve: CVE-2015-1735
cve: CVE-2015-1736
cve: CVE-2015-1737
cve: CVE-2015-1739
cve: CVE-2015-1740
cve: CVE-2015-1741
cve: CVE-2015-1742
cve: CVE-2015-1743
cve: CVE-2015-1744
cve: CVE-2015-1745
cve: CVE-2015-1747
cve: CVE-2015-1748
cve: CVE-2015-1750
cve: CVE-2015-1751
cve: CVE-2015-1752
cve: CVE-2015-1753
cve: CVE-2015-1754
cve: CVE-2015-1755
cve: CVE-2015-1765
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2015-1766
url: https://support.microsoft.com/en-us/kb/3058515
url: http://www.securityfocus.com/bid/74974
url: http://www.securityfocus.com/bid/74982
url: http://www.securityfocus.com/bid/74985
url: http://www.securityfocus.com/bid/74986
url: http://www.securityfocus.com/bid/74988
url: http://www.securityfocus.com/bid/74990
url: http://www.securityfocus.com/bid/74991
url: https://technet.microsoft.com/en-us/library/security/MS15-056
cert-bund: CB-K15/0782
dfn-cert: DFN-CERT-2015-0824
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3116180)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-124.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: 8.0.7601.17000 - 8.0.7601.19057
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code, gain access to sensitive information, elevate privileges, bypass certain security restrictions and execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors caused by improperly accessing objects in memory.
- Multiple XSS filter bypass errors.
- An error in VBScript which improperly discloses the contents of its memory.
- An error in the way that the VBScript engine renders when handling objects in memory in Internet Explorer.
- An error when Internet Explorer does not properly enforce content types.
- An error when Internet Explorer improperly discloses the contents of its memory.

... continues on next page ...

... continued from previous page ...

- An error when Internet Explorer fails to use the Address Space Layout Randomization (ASLR) security feature.
- An error when Internet Explorer does not properly enforce cross-domain policies.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3116180)`
OID:1.3.6.1.4.1.25623.1.0.806646
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-6083
cve: CVE-2015-6134
cve: CVE-2015-6135
cve: CVE-2015-6136
cve: CVE-2015-6138
cve: CVE-2015-6139
cve: CVE-2015-6140
cve: CVE-2015-6141
cve: CVE-2015-6142
cve: CVE-2015-6143
cve: CVE-2015-6144
cve: CVE-2015-6145
cve: CVE-2015-6146
cve: CVE-2015-6147
cve: CVE-2015-6148
cve: CVE-2015-6149
cve: CVE-2015-6150
cve: CVE-2015-6151
cve: CVE-2015-6152
cve: CVE-2015-6153
cve: CVE-2015-6154
cve: CVE-2015-6155
cve: CVE-2015-6156
cve: CVE-2015-6157
cve: CVE-2015-6158
cve: CVE-2015-6159
cve: CVE-2015-6160
cve: CVE-2015-6161
cve: CVE-2015-6162
cve: CVE-2015-6164
url: https://support.microsoft.com/en-us/kb/3116180
url: https://support.microsoft.com/en-us/kb/3104002
url: https://technet.microsoft.com/library/security/MS15-124
cert-bund: CB-K15/1804
cert-bund: CB-K15/1798
cert-bund: CB-K15/1794
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-1903
dfn-cert: DFN-CERT-2015-1893
dfn-cert: DFN-CERT-2015-1890
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3104517)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-112.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: 8.0.7601.17000 - 8.0.7601.19037
```

Impact
Successful exploitation will allow remote attackers to gain access to sensitive information, bypass security restrictions, corrupt memory and potentially execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to:
- Multiple improper memory object handling errors.
- An error in the way that the JScript and VBScript engines render when handling objects in memory in Internet Explorer

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3104517)`
OID:1.3.6.1.4.1.25623.1.0.805773
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2427
cve: CVE-2015-6064
cve: CVE-2015-6065
cve: CVE-2015-6066
cve: CVE-2015-6068
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-6069
cve: CVE-2015-6070
cve: CVE-2015-6071
cve: CVE-2015-6072
cve: CVE-2015-6073
cve: CVE-2015-6074
cve: CVE-2015-6075
cve: CVE-2015-6076
cve: CVE-2015-6077
cve: CVE-2015-6078
cve: CVE-2015-6079
cve: CVE-2015-6080
cve: CVE-2015-6081
cve: CVE-2015-6082
cve: CVE-2015-6084
cve: CVE-2015-6085
cve: CVE-2015-6086
cve: CVE-2015-6087
cve: CVE-2015-6088
cve: CVE-2015-6089
url: https://support.microsoft.com/en-us/kb/3104517
url: https://technet.microsoft.com/en-us/library/security/MS15-112
cert-bund: CB-K15/1658
cert-bund: CB-K15/1650
dfn-cert: DFN-CERT-2015-1741
dfn-cert: DFN-CERT-2015-1739
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3076321)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-065.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

. . . continues on next page . . .

... continued from previous page ...

Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x and VBScript 5.8 on 8.x/9.x/10.x/11.x.

Vulnerability Insight

Multiple flaws are due to improper handling memory objects when accessing it and does not properly validate permissions under specific conditions.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3076321)`

OID:1.3.6.1.4.1.25623.1.0.805720

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1729
cve: CVE-2015-1733
cve: CVE-2015-1767
cve: CVE-2015-2372
cve: CVE-2015-2383
cve: CVE-2015-2384
cve: CVE-2015-2385
cve: CVE-2015-2389
cve: CVE-2015-2390
cve: CVE-2015-2391
cve: CVE-2015-2397
cve: CVE-2015-2398
cve: CVE-2015-2401
cve: CVE-2015-2402
cve: CVE-2015-2403
cve: CVE-2015-2404
cve: CVE-2015-2388
cve: CVE-2015-2406
cve: CVE-2015-2408
cve: CVE-2015-2410
cve: CVE-2015-2411
cve: CVE-2015-2412
cve: CVE-2015-2413
cve: CVE-2015-2414
cve: CVE-2015-2419
cve: CVE-2015-2421
cve: CVE-2015-2422
cve: CVE-2015-2425
cve: CVE-2015-1738
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3065822
url: https://technet.microsoft.com/en-us/library/security/MS15-065
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K15/1014
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1062
dfn-cert: DFN-CERT-2015-1060
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3089548)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-094.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: 8.0.7601.17000 - 8.0.7601.18968
```

Impact
Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to:
- Multiple improper handling memory objects,
- Improper permissions validation, allowing a script to be run with elevated privileges.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3089548)`
OID:1.3.6.1.4.1.25623.1.0.805736
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2483
cve: CVE-2015-2484
cve: CVE-2015-2485
cve: CVE-2015-2486
cve: CVE-2015-2487
cve: CVE-2015-2489
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-2490
cve: CVE-2015-2491
cve: CVE-2015-2492
cve: CVE-2015-2493
cve: CVE-2015-2494
cve: CVE-2015-2498
cve: CVE-2015-2499
cve: CVE-2015-2500
cve: CVE-2015-2501
cve: CVE-2015-2541
cve: CVE-2015-2542
url: https://support.microsoft.com/en-us/kb/3089548
url: https://technet.microsoft.com/en-us/library/security/MS15-094
cert-bund: CB-K15/1323
cert-bund: CB-K15/1314
dfn-cert: DFN-CERT-2015-1391
dfn-cert: DFN-CERT-2015-1384
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3082442)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-079.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to:
- Multiple improper handling memory objects,
- Fails to use ASLR security feature, allowing an attacker to more reliably predict the memory offsets of specific instructions.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3082442)`
OID:1.3.6.1.4.1.25623.1.0.805731
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2423
cve: CVE-2015-2441
cve: CVE-2015-2442
cve: CVE-2015-2443
cve: CVE-2015-2444
cve: CVE-2015-2445
cve: CVE-2015-2446
cve: CVE-2015-2447
cve: CVE-2015-2448
cve: CVE-2015-2449
cve: CVE-2015-2450
cve: CVE-2015-2451
cve: CVE-2015-2452
url: https://support.microsoft.com/en-us/kb/3082442
url: http://www.securityfocus.com/bid/76202
url: http://www.securityfocus.com/bid/76197
url: http://www.securityfocus.com/bid/76196
url: http://www.securityfocus.com/bid/76195
url: http://www.securityfocus.com/bid/76194
url: http://www.securityfocus.com/bid/76198
url: http://www.securityfocus.com/bid/76193
url: http://www.securityfocus.com/bid/76192
url: http://www.securityfocus.com/bid/76191
url: http://www.securityfocus.com/bid/76199
url: http://www.securityfocus.com/bid/76190
url: http://www.securityfocus.com/bid/76189
url: http://www.securityfocus.com/bid/76188
url: https://technet.microsoft.com/en-us/library/security/MS15-079
cert-bund: CB-K15/1174
cert-bund: CB-K15/1172
cert-bund: CB-K15/1170
cert-bund: CB-K15/1169
dfn-cert: DFN-CERT-2015-1236
dfn-cert: DFN-CERT-2015-1235
dfn-cert: DFN-CERT-2015-1232
dfn-cert: DFN-CERT-2015-1231
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3049563)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-043.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow context
- dependent attacker to corrupt memory, execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to:
- Multiple unspecified flaws in VBScript and JScript that may allow a context-dependent attacker to bypass Address Space Layout Randomization (ASLR).
- an unspecified flaw that may allow a context-dependent attacker to bypass unspecified features and execute code through the use of another vulnerability with higher privileges than would normally be allowed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3049563)`
OID:1.3.6.1.4.1.25623.1.0.805380
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-1658
cve: CVE-2015-1684
cve: CVE-2015-1685
cve: CVE-2015-1686
cve: CVE-2015-1688
cve: CVE-2015-1689
cve: CVE-2015-1691
cve: CVE-2015-1692
cve: CVE-2015-1694
cve: CVE-2015-1703
cve: CVE-2015-1704
cve: CVE-2015-1705
cve: CVE-2015-1706
cve: CVE-2015-1708
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-1709
cve: CVE-2015-1710
cve: CVE-2015-1711
cve: CVE-2015-1712
cve: CVE-2015-1713
cve: CVE-2015-1714
cve: CVE-2015-1717
cve: CVE-2015-1718
url: https://support.microsoft.com/kb/3049563
url: https://technet.microsoft.com/library/security/MS15-043
cert-bund: CB-K15/0668
cert-bund: CB-K15/0660
dfn-cert: DFN-CERT-2015-0689
dfn-cert: DFN-CERT-2015-0681
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3008923)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-080.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, bypass certain security restrictions, and compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Flaws are due to multiple unspecified vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3008923)`
OID:1.3.6.1.4.1.25623.1.0.805112
Version used: `2023-07-27T05:05:08Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-6327
cve: CVE-2014-6329
cve: CVE-2014-6330
cve: CVE-2014-6366
cve: CVE-2014-6369
cve: CVE-2014-6373
cve: CVE-2014-6374
cve: CVE-2014-6375
cve: CVE-2014-6376
cve: CVE-2014-8966
url: https://support.microsoft.com/kb/3008923
url: http://www.securityfocus.com/bid/71446
url: http://www.securityfocus.com/bid/71447
url: http://www.securityfocus.com/bid/71448
url: http://www.securityfocus.com/bid/71450
url: http://www.securityfocus.com/bid/71452
url: http://www.securityfocus.com/bid/71453
url: http://www.securityfocus.com/bid/71454
url: http://www.securityfocus.com/bid/71455
url: http://www.securityfocus.com/bid/71456
url: http://www.securityfocus.com/bid/71457
url: https://technet.microsoft.com/library/security/ms14-080
cert-bund: CB-K14/1523
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3003057)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-065.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, bypass certain security restrictions, and compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Flaws are due to multiple unspecified vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3003057)`

OID:1.3.6.1.4.1.25623.1.0.804790

Version used: `2023-07-27T05:05:08Z`

References

```
cve: CVE-2014-4143
cve: CVE-2014-6323
cve: CVE-2014-6337
cve: CVE-2014-6339
cve: CVE-2014-6340
cve: CVE-2014-6341
cve: CVE-2014-6342
cve: CVE-2014-6343
cve: CVE-2014-6344
cve: CVE-2014-6345
cve: CVE-2014-6346
cve: CVE-2014-6347
cve: CVE-2014-6348
cve: CVE-2014-6349
cve: CVE-2014-6350
cve: CVE-2014-6351
cve: CVE-2014-6353
url: https://support.microsoft.com/kb/3003057
url: http://www.securityfocus.com/bid/70323
url: http://www.securityfocus.com/bid/70333
url: http://www.securityfocus.com/bid/70337
url: http://www.securityfocus.com/bid/70338
url: http://www.securityfocus.com/bid/70341
url: http://www.securityfocus.com/bid/70344
url: http://www.securityfocus.com/bid/70345
url: http://www.securityfocus.com/bid/70346
url: http://www.securityfocus.com/bid/70347
url: http://www.securityfocus.com/bid/70348
url: http://www.securityfocus.com/bid/70939
url: http://www.securityfocus.com/bid/70940
url: http://www.securityfocus.com/bid/70941
url: http://www.securityfocus.com/bid/70942
url: http://www.securityfocus.com/bid/70946
url: http://www.securityfocus.com/bid/70947
url: http://www.securityfocus.com/bid/70948
url: https://technet.microsoft.com/library/security/MS14-065
cert-bund: CB-K14/1402
cert-bund: CB-K14/1401
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (2962482)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-029.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to corrupt memory by the execution of arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple unspecified flaws are due to user-supplied input is not properly sanitized.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (2962482)`
OID:1.3.6.1.4.1.25623.1.0.804579
Version used: `2023-07-27T05:05:08Z`

References

```
cve: CVE-2014-0310
cve: CVE-2014-1815
url: https://support.microsoft.com/kb/2953522
url: http://www.securityfocus.com/bid/67299
url: http://www.securityfocus.com/bid/67301
url: https://support.microsoft.com/kb/2961851
url: https://technet.microsoft.com/library/security/ms14-029
cert-bund: CB-K14/0564
```

High (CVSS: 9.3)
NVT: Microsoft Windows Font Drivers Remote Code Execution Vulnerability (3057110)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-044.

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow an attacker to gain access to potentially sensitive information and to execute arbitrary code on the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2

Vulnerability Insight

The flaw exists due to improper handling of TrueType fonts and OpenType fonts.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Font Drivers Remote Code Execution Vulnerability (3057110)`

OID:1.3.6.1.4.1.25623.1.0.805556

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1670
cve: CVE-2015-1671
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3045171
url: http://www.securityfocus.com/bid/74490
url: http://www.securityfocus.com/bid/74485
url: https://technet.microsoft.com/library/security/MS15-044
cert-bund: CB-K15/0668
dfn-cert: DFN-CERT-2015-0689
```

High (CVSS: 9.3)

NVT: Microsoft Windows Data Access Components Remote Code Execution Vulnerability (2698365)

... continues on next page ...

. . . continued from previous page . . .

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-045.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to gain sensitive information or execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Vulnerability is due to the way that Microsoft Data Access Components accesses an object in memory that has been improperly initialized when parsing XML code.

Vulnerability Detection Method
Details: `Microsoft Windows Data Access Components Remote Code Execution Vulnerability (2.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902687
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-1891
url: http://support.microsoft.com/kb/2698365
url: http://www.securityfocus.com/bid/54308
url: http://www.securitytracker.com/id/1027227
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-045
dfn-cert: DFN-CERT-2012-1329
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Multiple Vulnerabilities (2916607)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-009.

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.dll
File version:     0
Vulnerable range: 2.0.50727.5400 - 2.0.50727.5478
```

Impact
Successful exploitation could allow an attacker to bypass certain security mechanism and cause denial of service.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 1.0, 1.1, 2.0, 3.0, 3.5, 3.5.1, 4.0, 4.5 and 4.5.1.

Vulnerability Insight
Multiple flaws due to:
- ASP.NET does not properly identify stale HTTP connections.
- An error within the .NET framework when handling certain COM objects.
- Additionally, some unspecified weakness exists.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Multiple Vulnerabilities (2916607)`
OID:1.3.6.1.4.1.25623.1.0.903337
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2014-0253
cve: CVE-2014-0257
cve: CVE-2014-0295
url: http://support.microsoft.com/kb/2916607
url: http://www.securityfocus.com/bid/65415
url: http://www.securityfocus.com/bid/65417
url: http://www.securityfocus.com/bid/65418
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-009
cert-bund: CB-K14/0169
```

High (CVSS: 9.3)
NVT: Microsoft ASP.NET Insecure Site Configuration Vulnerability (2905247)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing an important security update according to Microsoft advisory (2905247).

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to use specially crafted HTTP content to inject code to be run in the context of the service account on the ASP.NET server.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework versions 1.1, 2.0, 3.5, 3.5.1, 4.0, 4.5 and 4.5.1.

Vulnerability Insight
Flaw is due to the view state that exists when Machine Authentication Code (MAC) validation is disabled through configuration settings.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft ASP.NET Insecure Site Configuration Vulnerability (2905247)`
OID:1.3.6.1.4.1.25623.1.0.804038
Version used: `2023-07-27T05:05:08Z`

References
```
url: http://support.microsoft.com/kb/2905247
url: https://technet.microsoft.com/en-us/security/advisory/2905247
```

High (CVSS: 9.3)
NVT: Microsoft Windows DirectPlay Remote Code Execution Vulnerability (2770660)

Summary
This host is missing an important security update according to Microsoft Bulletin MS12-082.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to execute arbitrary code by tricking a user into opening a malicious office document.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

The vulnerability is caused when Windows DirectPlay fails to properly handle specially crafted office document with embedded content.

Vulnerability Detection Method

Details: `Microsoft Windows DirectPlay Remote Code Execution Vulnerability (2770660)`
OID:1.3.6.1.4.1.25623.1.0.901212
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-1537
url: http://support.microsoft.com/kb/2770660
url: http://www.securityfocus.com/bid/56839
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-082
dfn-cert: DFN-CERT-2012-2232
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Multiple Vulnerabilities (2916607)

Summary

This host is missing an important security update according to Microsoft Bulletin MS14-009.

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v2.0.50727\System.Web.dll
File version:     0
Vulnerable range: 2.0.50727.5400 - 2.0.50727.5478
```

Impact

Successful exploitation could allow an attacker to bypass certain security mechanism and cause denial of service.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 1.0, 1.1, 2.0, 3.0, 3.5, 3.5.1, 4.0, 4.5 and 4.5.1.

Vulnerability Insight
Multiple flaws due to:
- ASP.NET does not properly identify stale HTTP connections.
- An error within the .NET framework when handling certain COM objects.
- Additionally, some unspecified weakness exists.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Multiple Vulnerabilities (2916607)`
OID:1.3.6.1.4.1.25623.1.0.903337
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2014-0253
cve: CVE-2014-0257
cve: CVE-2014-0295
url: http://support.microsoft.com/kb/2916607
url: http://www.securityfocus.com/bid/65415
url: http://www.securityfocus.com/bid/65417
url: http://www.securityfocus.com/bid/65418
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-009
cert-bund: CB-K14/0169
```

High (CVSS: 9.3)
NVT: Microsoft EAP Implementation TLS Information Disclosure Vulnerability (2977292)

Summary
This host is missing an important security update according to Microsoft Security Advisory 2977292.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation allows an attacker to perform man-in-the-middle attacks and recover plaintext from encrypted sessions.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2

Vulnerability Insight

The error exists due to use of lower versions of TLS allowing recovery of plaintext from encrypted sessions.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft EAP Implementation TLS Information Disclosure Vulnerability (2977292)`
OID:1.3.6.1.4.1.25623.1.0.804869
Version used: `2023-07-26T05:05:09Z`

References

```
url: https://support.microsoft.com/kb/2977292
url: https://technet.microsoft.com/en-US/library/security/2977292
```

High (CVSS: 9.3)
NVT: Microsoft Windows XML Core Services Remote Code Execution Vulnerability (2993958)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS14-067.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to compromise a vulnerable system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight

The flaw is due to an unspecified error when parsing XML content.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows XML Core Services Remote Code Execution Vulnerability (299395.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.804879

Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-4118
url: https://support.microsoft.com/kb/2993958
url: http://www.securityfocus.com/bid/70957
url: https://technet.microsoft.com/library/security/MS14-067
cert-bund: CB-K14/1402
```

High (CVSS: 9.3)

NVT: Microsoft Windows VBScript Remote Code Execution Vulnerability (3072604)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-066.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code and corrupt memory.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Flaw exists due to error in VBScript that is triggered as user-supplied input is not properly validated.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows VBScript Remote Code Execution Vulnerability (3072604)`

OID:1.3.6.1.4.1.25623.1.0.805076

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2372
url: https://support.microsoft.com/en-us/kb/3072604
url: https://technet.microsoft.com/en-us/library/security/MS15-066
url: https://technet.microsoft.com/library/security/MS15-066
cert-bund: CB-K15/1014
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1062
dfn-cert: DFN-CERT-2015-1060
```

High (CVSS: 9.3)

NVT: Microsoft Windows VBScript Remote Code Execution Vulnerability (3016711)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS14-084.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code and corrupt memory.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The flaw is due to error in Microsoft VBScript Engine triggered when user-supplied input is not properly sanitized.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows VBScript Remote Code Execution Vulnerability (3016711)`

OID:1.3.6.1.4.1.25623.1.0.805206

Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-6363
url: https://support.microsoft.com/kb/3016711
url: http://www.securityfocus.com/bid/71504
url: https://support.microsoft.com/kb/3012168
url: https://support.microsoft.com/kb/3012172
url: https://support.microsoft.com/kb/3012176
url: https://technet.microsoft.com/library/security/ms14-084
url: https://technet.microsoft.com/library/security/MS14-084
cert-bund: CB-K14/1525
cert-bund: CB-K14/1523
```

High (CVSS: 9.3)
NVT: Microsoft Windows Shell Remote Code Execution Vulnerability (2691442)

Summary

This host is missing an important security update according to Microsoft Bulletin MS12-048.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow an attacker to execute arbitrary shell commands with user level privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

The vulnerability is caused when Windows shell does not properly handle specially crafted file or directory names.

Vulnerability Detection Method

Details: `Microsoft Windows Shell Remote Code Execution Vulnerability (2691442)`

OID:1.3.6.1.4.1.25623.1.0.902845

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-0175
url: http://support.microsoft.com/kb/2691442
url: http://www.securityfocus.com/bid/54307
url: http://www.securitytracker.com/id/1027230
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-048
dfn-cert: DFN-CERT-2012-1331
```

High (CVSS: 9.3)

NVT: Microsoft Windows Shell and Tablet Input Band Remote Code Execution Vulnerabilities (3096443)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-109.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Shell32.dll
File version:     6.1.7601.17514
Vulnerable range: Version Less than - 6.1.7601.18952
```

Impact

Successful exploitation will allow an attacker to conduct denial-of-service conditions and execute arbitrary code in the context of the currently logged-in user.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2012
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012R2
- Microsoft Windows 8/8.1 x32/x64

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

Multiple flaws are due to:
- Windows Shell fails to properly handle objects in memory.
- Tablet Input Band fails to properly handle objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Shell and Tablet Input Band Remote Code Execution Vulnerabili.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.806090

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2515
cve: CVE-2015-2548
url: https://support.microsoft.com/en-us/kb/3096443
url: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms
↪15-109
cert-bund: CB-K15/1507
dfn-cert: DFN-CERT-2015-1586
```

High (CVSS: 9.3)

NVT: Microsoft .NET Framework 'RC4' Information Disclosure Vulnerability (2960358)

Summary

This host is missing an important security update according to Microsoft Security Advisory 2960358.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow an attacker to perform man-in-the-middle attacks and recover plaintext from encrypted sessions.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Microsoft .NET Framework 3.5, 3.5.1, 4.0 and 4.5 and 4.5.X.

Vulnerability Insight

The flaw is due to the RC4 encryption algorithm is used in Transport Layer Security (TLS).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework 'RC4' Information Disclosure Vulnerability (2960358)`

OID:1.3.6.1.4.1.25623.1.0.804587

Version used: `2023-07-27T05:05:08Z`

References

```
url: https://support.microsoft.com/kb/2960358
url: https://technet.microsoft.com/en-us/library/security/2960358
```

High (CVSS: 9.3)
NVT: Microsoft Windows DirectWrite Remote Code Execution Vulnerabilities (2848295)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS13-054.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow attackers to execute arbitrary code as the logged-on use.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

The flaw is due to an error when processing TrueType fonts and can be exploited to cause a buffer overflow via a specially crafted file.

Vulnerability Detection Method

Details: `Microsoft Windows DirectWrite Remote Code Execution Vulnerabilities (2848295)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.902983
Version used: 2022-04-25T14:50:49Z

References

```
cve: CVE-2013-3129
url: http://support.microsoft.com/kb/2835361
url: http://www.securityfocus.com/bid/60978
url: http://www.securitytracker.com/id/1028750
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-054
dfn-cert: DFN-CERT-2013-1267
dfn-cert: DFN-CERT-2013-1264
dfn-cert: DFN-CERT-2013-1262
```

High (CVSS: 9.3)
NVT: Microsoft Windows Scripting Runtime Object Library RCE Vulnerability (2909158)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS13-099.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to execute arbitrary code, cause a DoS (Denial of Service), and compromise the vulnerable system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The flaw is due to memory corruption resulting from improperly handling of an object in memory by Scripting Runtime Object Library.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Scripting Runtime Object Library RCE Vulnerability (2909158)`

OID:1.3.6.1.4.1.25623.1.0.903505

Version used: `2022-07-26T10:10:42Z`

References

```
cve: CVE-2013-5056
url: http://support.microsoft.com/kb/2892074
url: http://www.securityfocus.com/bid/64082
url: http://support.microsoft.com/kb/2892075
url: http://support.microsoft.com/kb/2892076
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-099
cert-bund: CB-K13/1027
dfn-cert: DFN-CERT-2013-2048
```

High (CVSS: 9.3)
NVT: Microsoft Windows Remote Code Execution Vulnerabilities (3105864)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-115.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19045
```

Impact

Successful exploitation will allow an attacker to do Kernel Address Space Layout Randomization (KASLR) bypass and execute arbitrary code taking complete control of the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8/8.1 x32/x64
- Microsoft Edge on Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight

Multiple flaws exist due to:

- The way that Windows handles objects in memory. An attacker who successfully exploited the vulnerabilities could run arbitrary code in kernel mode.
- The Windows fails to properly initialize memory addresses, allowing an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass.
- The Adobe Type Manager Library in Windows improperly handles specially crafted embedded fonts.
- The Windows kernel fails to properly validate permissions, allowing an attacker to inappropriately interact with the filesystem from low integrity level user-mode applications.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Remote Code Execution Vulnerabilities (3105864)`
OID:1.3.6.1.4.1.25623.1.0.806157
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-6100
cve: CVE-2015-6101
cve: CVE-2015-6102
cve: CVE-2015-6103
cve: CVE-2015-6104
cve: CVE-2015-6109
cve: CVE-2015-6113
url: https://support.microsoft.com/en-us/kb/3097877
url: https://support.microsoft.com/en-us/kb/3101746
url: https://technet.microsoft.com/library/security/ms15-115
cert-bund: CB-K15/1649
dfn-cert: DFN-CERT-2015-1742
```

High (CVSS: 9.3)
NVT: Microsoft Adobe Font Driver Remote Code Execution Vulnerabilities (3032323)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-021.

Vulnerability Detection Result

```
Installed version: 5.1.2.230
Fixed version:     5.1.2.241
Installation
path / port:       C:\Windows
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to execute arbitrary code with kernel-mode privileges and take complete control of the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight

Multiple flaws are exists in how the Adobe Font Driver manages memory when parsing fonts. The vulnerabilities are caused when the Adobe Font Driver improperly overwrites objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Adobe Font Driver Remote Code Execution Vulnerabilities (3032323)`

OID:1.3.6.1.4.1.25623.1.0.805052

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0074
cve: CVE-2015-0087
cve: CVE-2015-0088
cve: CVE-2015-0089
cve: CVE-2015-0090
cve: CVE-2015-0091
cve: CVE-2015-0092
cve: CVE-2015-0093
url: https://support.microsoft.com/kb/3032323
url: https://technet.microsoft.com/library/security/MS15-021
cert-bund: CB-K15/0319
dfn-cert: DFN-CERT-2015-0324
```

High (CVSS: 9.3)
NVT: Microsoft Windows Remote Code Execution Vulnerabilities (3041836)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-020.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to run arbitrary code and take complete control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Multiple flaws are exists when,
- Windows Text Services improperly handles objects in memory and
- Microsoft Windows improperly handles the loading of DLL files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Remote Code Execution Vulnerabilities (3041836)`
OID:1.3.6.1.4.1.25623.1.0.805053
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-0081
cve: CVE-2015-0096
url: http://www.securitytracker.com/id/1031890
url: https://support.microsoft.com/kb/3033889
url: https://support.microsoft.com/kb/3039066
url: https://technet.microsoft.com/library/security/MS15-020
cert-bund: CB-K15/0319
dfn-cert: DFN-CERT-2015-0324
```

High (CVSS: 9.3)
NVT: Microsoft Windows Privilege Elevation Vulnerabilities (3060716)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-090.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow users to gain privileges via a crafted application.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
An elevation of privilege vulnerabilities are exists in Windows Object Manager when it,
- Fails to properly validate and enforce impersonation levels.
- Improperly allows certain registry interactions from within vulnerable sandboxed applications.
- Improperly allows certain filesystem interactions from within vulnerable sandboxed applications.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Privilege Elevation Vulnerabilities (3060716)`
OID:1.3.6.1.4.1.25623.1.0.805094
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2428
cve: CVE-2015-2429
cve: CVE-2015-2430
url: https://support.microsoft.com/en-us/kb/3060716
url: http://www.securityfocus.com/bid/76227
url: http://www.securityfocus.com/bid/76231
url: http://www.securityfocus.com/bid/76233
url: https://technet.microsoft.com/library/security/MS15-090
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K15/1174
dfn-cert: DFN-CERT-2015-1236
```

High (CVSS: 9.3)
NVT: Windows OLE Object Handling Arbitrary Code Execution Vulnerability (3000869)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-060.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attacker to compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
The flaw is due to an unspecified error when handling OLE objects embedded within Microsoft Office files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Windows OLE Object Handling Arbitrary Code Execution Vulnerability (3000869)`
OID:1.3.6.1.4.1.25623.1.0.804860
Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-4114
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/3000869
url: http://www.securityfocus.com/bid/70419
url: https://technet.microsoft.com/library/security/ms14-060
```

. . . continues on next page . . .

. . . continued from previous page . . .

cert-bund: CB-K14/1291

High (CVSS: 9.3)
NVT: Microsoft Windows OLE Object Handling Code Execution Vulnerabilities (3011443)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-064.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attacker to execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
A flaw exists due to unspecified errors when handling OLE objects within Microsoft Office files and Internet Explorer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows OLE Object Handling Code Execution Vulnerabilities (3011443)`
OID:1.3.6.1.4.1.25623.1.0.805015
Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-6332
cve: CVE-2014-6352
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/3011443
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/70690
url: http://www.securityfocus.com/bid/70952
url: https://support.microsoft.com/kb/3010788
url: https://support.microsoft.com/kb/3006226
url: https://technet.microsoft.com/library/security/ms14-064
cert-bund: CB-K14/1402
cert-bund: CB-K14/1321
```

High (CVSS: 9.3)
NVT: Microsoft Windows OLE Object Handling Code Execution Vulnerabilities (3011443)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-064.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attacker to execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
A flaw exists due to unspecified errors when handling OLE objects within Microsoft Office files and Internet Explorer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows OLE Object Handling Code Execution Vulnerabilities (3011443)`
OID:1.3.6.1.4.1.25623.1.0.805015
Version used: `2023-07-26T05:05:09Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2014-6332
cve: CVE-2014-6352
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/3011443
url: http://www.securityfocus.com/bid/70690
url: http://www.securityfocus.com/bid/70952
url: https://support.microsoft.com/kb/3010788
url: https://support.microsoft.com/kb/3006226
url: https://technet.microsoft.com/library/security/ms14-064
cert-bund: CB-K14/1402
cert-bund: CB-K14/1321
```

High (CVSS: 9.3)
NVT: Microsoft XML Core Services Remote Code Execution Vulnerability (2719615)

Summary

Microsoft XML Core Services is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Msxml6.dll
File version:     6.30.7601.17514
Vulnerable range: 6.30.7601.17000 - 6.30.7601.17856
```

Impact

Successful exploitation could allow remote attackers to execute arbitrary code as the logged-on user.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

- Microsoft Expression Web 2
- Microsoft Office Word Viewer
- Microsoft Office Compatibility
- Microsoft Office 2003 Service Pack 3 and prior
- Microsoft Office 2007 Service Pack 3 and prior
- Microsoft Expression Web Service Pack 1 and prior
- Microsoft Groove Server 2007 Service Pack 3 and prior
- Microsoft SharePoint Server 2007 Service Pack 3 and prior
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

Microsoft XML Core Services attempts to access an object in memory that has not been initialized, which allows an attacker to corrupt memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft XML Core Services Remote Code Execution Vulnerability (2719615)`

OID:1.3.6.1.4.1.25623.1.0.802864

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2012-1889
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://securitytracker.com/id/1027157
url: http://support.microsoft.com/kb/2719615
url: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2012/2
↪719615
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-043
dfn-cert: DFN-CERT-2012-1327
dfn-cert: DFN-CERT-2012-1125
```

High (CVSS: 9.3)
NVT: Microsoft XML Core Services Remote Code Execution Vulnerabilities (2756145)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS13-002.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Msxml6.dll
File version:     0
Vulnerable range: 6.30.7601.17000 - 6.30.7601.17987
```

Impact

Successful exploitation could allow remote attackers to execute arbitrary code as the logged-on user.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

- Microsoft Expression Web 2
- Microsoft Office Word Viewer
- Microsoft Office Compatibility
- Microsoft Office 2003 Service Pack 3 and prior
- Microsoft Office 2007 Service Pack 3 and prior
- Microsoft XML Core Services 3.0, 4.0, 5.0 and 6.0
- Microsoft Expression Web Service Pack 1 and prior
- Microsoft Groove Server 2007 Service Pack 3 and prior
- Microsoft SharePoint Server 2007 Service Pack 3 and prior
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

Integer truncation and an unspecified error caused due to the way that Microsoft XML Core Services parses XML content.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft XML Core Services Remote Code Execution Vulnerabilities (2756145)`

OID:1.3.6.1.4.1.25623.1.0.903101

Version used: `2022-04-25T14:50:49Z`

References

```
cve: CVE-2013-0006
cve: CVE-2013-0007
url: http://xforce.iss.net/xforce/xfdb/80873
url: http://www.securityfocus.com/bid/57116
url: http://www.securityfocus.com/bid/57122
url: http://xforce.iss.net/xforce/xfdb/80875
url: http://support.microsoft.com/kb/2756145
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-002
dfn-cert: DFN-CERT-2013-0044
```

High (CVSS: 9.3)

NVT: Microsoft Font Driver Remote Code Execution Vulnerability (3079904)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing a critical security update according to Microsoft Bulletin MS15-078.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Atmfd.dll
File version:     5.1.2.230
Vulnerable range: Less than 5.1.2.243
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code. Failed exploit attempts will result in a denial-of-service condition.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight

The flaw is due to the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Font Driver Remote Code Execution Vulnerability (3079904)`
OID:1.3.6.1.4.1.25623.1.0.805726
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2426
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3079904
url: http://www.securityfocus.com/bid/75951
url: https://technet.microsoft.com/library/security/MS15-078
cert-bund: CB-K15/1037
dfn-cert: DFN-CERT-2015-1094
```

High (CVSS: 9.3)
NVT: Microsoft Windows Components Privilege Elevation Vulnerability (3025421)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-005.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to gain restricted privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
The flaw is due to an error when handling directory traversal sequences within the TS WebProxy Windows component, which can be exploited to gain otherwise restricted privileges.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Components Privilege Elevation Vulnerability (3025421)`
OID:1.3.6.1.4.1.25623.1.0.805037
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-0016
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/3025421
url: http://www.securityfocus.com/bid/71965
url: https://technet.microsoft.com/library/security/MS15-004
cert-bund: CB-K15/0038
dfn-cert: DFN-CERT-2015-0036
```

High (CVSS: 9.3)
NVT: Microsoft Graphics Component Remote Code Executioon Vulnerabilities (3078662)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-080.

Vulnerability Detection Result

```
Installed version: 5.1.2.230
Fixed version:     5.1.2.244
Installation
path / port:       C:\Windows
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code. Failed exploit attempts will result in a denial-of-service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
The flaw is due to the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Graphics Component Remote Code Executioon Vulnerabilities (3078662)`
OID:1.3.6.1.4.1.25623.1.0.805081
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2432
cve: CVE-2015-2458
cve: CVE-2015-2459
cve: CVE-2015-2460
cve: CVE-2015-2461
cve: CVE-2015-2462
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-2435
cve: CVE-2015-2455
cve: CVE-2015-2456
cve: CVE-2015-2463
cve: CVE-2015-2464
cve: CVE-2015-2433
cve: CVE-2015-2453
cve: CVE-2015-2454
cve: CVE-2015-2465
url: https://support.microsoft.com/en-us/kb/3078662
url: https://technet.microsoft.com/library/security/MS15-080
cert-bund: CB-K15/1174
cert-bund: CB-K15/1172
dfn-cert: DFN-CERT-2015-1236
dfn-cert: DFN-CERT-2015-1235
```

High (CVSS: 9.3)
NVT: Microsoft VBScript Remote Code Execution Vulnerability (2928390)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-011.

Vulnerability Detection Result

```
Vulnerable range:  < 5.8.7601.18337, 5.8.7601.22000 - 5.8.7601.22534
File checked:      C:\Windowssystem32\Vbscript.dll
File version:      5.8.7601.17514
```

Impact
Successful exploitation will allow attackers to execute arbitrary code and corrupt memory.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 2003 x32 Pack 3 and prior
- Microsoft Windows 2003 x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64

. . . continues on next page . . .

... continued from previous page ...

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight

Flaw is due to improper handling of memory objects in VBScript engine.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft VBScript Remote Code Execution Vulnerability (2928390)`

OID:1.3.6.1.4.1.25623.1.0.903229

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2014-0271
url: http://support.microsoft.com/kb/2928390
url: http://www.securityfocus.com/bid/65395
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-011
cert-bund: CB-K14/0173
cert-bund: CB-K14/0168
```

High (CVSS: 9.3)

NVT: Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2870008)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS13-081

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\drivers\usbd.sys
File version:     6.1.7600.16385
Vulnerable range: Less than 6.1.7601.18251
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code with kernel-mode privileges and take complete control of the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior

... continues on next page ...

. . . continued from previous page . . .

- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

Multiple flaws exist due to:

- An error when parsing OpenType fonts (OTF) can be exploited to corrupt memory.
- An error when handling the USB descriptor of inserted USB devices can be exploited to corrupt memory.
- A use-after-free error within the kernel-mode driver (win32k.sys) can be exploited to gain escalated privileges.
- An error when handling objects in memory related to App Containers can be exploited to disclose information from a different App Container.
- An error related to NULL page handling within the kernel-mode driver (win32k.sys) can be exploited to gain escalated privileges.
- A double fetch error within the DirectX graphics kernel subsystem (dxgkrnl.sys) can be exploited to gain escalated privileges.
- An error when parsing the CMAP table while rendering TrueType fonts (TTF) can be exploited to corrupt memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (28.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.903500

Version used: `2022-07-26T10:10:42Z`

References

```
cve: CVE-2013-3128
cve: CVE-2013-3200
cve: CVE-2013-3879
cve: CVE-2013-3880
cve: CVE-2013-3881
cve: CVE-2013-3888
cve: CVE-2013-3894
url: http://support.microsoft.com/kb/2862330
url: http://www.securityfocus.com/bid/62819
url: http://www.securityfocus.com/bid/62821
url: http://www.securityfocus.com/bid/62823
url: http://www.securityfocus.com/bid/62828
url: http://www.securityfocus.com/bid/62830
url: http://www.securityfocus.com/bid/62831
url: http://www.securityfocus.com/bid/62833
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-081
cert-bund: CB-K13/0762
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K13/0760
dfn-cert: DFN-CERT-2013-1755
dfn-cert: DFN-CERT-2013-1753
```

High (CVSS: 9.3)
NVT: Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (2850851)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS13-053.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to cause a buffer overflow and execute arbitrary code with kernel privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to:
- Unspecified errors within the Windows kernel-mode driver (win32k.sys) when processing certain objects and can be exploited to cause a crash or execute arbitrary code with the kernel privilege.
- An error exists within the GDI+ subsystem.

Vulnerability Detection Method
Details: `Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (28.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902978
Version used: `2022-08-09T10:11:17Z`

. . . continues on next page . . .

... continued from previous page ...

References

```
cve: CVE-2013-1300
cve: CVE-2013-1340
cve: CVE-2013-1345
cve: CVE-2013-3129
cve: CVE-2013-3167
cve: CVE-2013-3172
cve: CVE-2013-3173
cve: CVE-2013-3660
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://support.microsoft.com/kb/2850851
url: http://www.securityfocus.com/bid/60051
url: http://www.securityfocus.com/bid/60946
url: http://www.securityfocus.com/bid/60947
url: http://www.securityfocus.com/bid/60948
url: http://www.securityfocus.com/bid/60949
url: http://www.securityfocus.com/bid/60950
url: http://www.securityfocus.com/bid/60951
url: http://www.securityfocus.com/bid/60978
url: http://www.securitytracker.com/id/1028746
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-053
dfn-cert: DFN-CERT-2013-1267
dfn-cert: DFN-CERT-2013-1264
dfn-cert: DFN-CERT-2013-1262
```

High (CVSS: 9.3)
NVT: Microsoft Windows Graphics Component Remote Code Execution Vulnerability (3089656)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-097.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.18985
```

Impact

Successful exploitation will allow an attacker to do Kernel Address Space Layout Randomization (KASLR) bypass and execute arbitrary code taking complete control of the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS

- Microsoft Windows 8/8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

Multiple flaws exist due to:

- An unspecified error in the Windows Adobe Type Manager Library which improperly handles specially crafted OpenType fonts.
- An unspecified error in Windows Adobe Type Manager Library which fails to properly handle objects in memory.
- Multiple errors in Windows kernel-mode driver which fails to properly handle objects in memory.
- An unspecified error in the Windows kernel mode driver (Win32k.sys) which fails to properly validate and enforce integrity levels during certain process initialization scenarios.
- An error in Windows kernel which fails to properly initialize a memory address.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Graphics Component Remote Code Execution Vulnerability (30896.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.805979

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2506
cve: CVE-2015-2507
cve: CVE-2015-2508
cve: CVE-2015-2510
cve: CVE-2015-2511
cve: CVE-2015-2512
cve: CVE-2015-2517
cve: CVE-2015-2518
cve: CVE-2015-2527
cve: CVE-2015-2529
cve: CVE-2015-2546
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3086255
url: https://support.microsoft.com/en-us/kb/3087039
url: https://support.microsoft.com/en-us/kb/3087135
url: https://technet.microsoft.com/library/security/ms15-097
cert-bund: CB-K15/1321
cert-bund: CB-K15/1319
```

... continues on next page ...

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2015-1386
dfn-cert: DFN-CERT-2015-1385

High (CVSS: 9.3)
NVT: Microsoft Windows Graphics Component Remote Code Execution Vulnerability (3046306)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-035.

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation will allow remote attackers to execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Flaw exists due to error that is triggered when handling a specially crafted enhanced metafile (EMF) image format file.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Microsoft Windows Graphics Component Remote Code Execution Vulnerability (30463.
↪..
OID:1.3.6.1.4.1.25623.1.0.805534
Version used: 2023-07-25T05:05:58Z

References
cve: CVE-2015-1645
url: https://support.microsoft.com/en-us/kb/3046306
url: https://technet.microsoft.com/library/security/MS15-035
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545

High (CVSS: 9.3)
NVT: Microsoft Windows Common Controls Remote Code Execution Vulnerability (3059317)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-060.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code within the context of the application that uses the ActiveX control.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
The flaw is due to Microsoft Common Controls, when it accesses an object in memory that has not been correctly initialized or has been deleted

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Common Controls Remote Code Execution Vulnerability (3059317)`
OID:1.3.6.1.4.1.25623.1.0.805399
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1756
url: https://support.microsoft.com/en-us/kb/3059317
url: http://www.securityfocus.com/bid/75017
url: https://technet.microsoft.com/en-us/library/security/MS15-060
cert-bund: CB-K15/0783
dfn-cert: DFN-CERT-2015-0827
```

High (CVSS: 9.3)
NVT: Microsoft Windows ActiveX Control RCE Vulnerability (2900986)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS13-090.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation allows execution of arbitrary code when viewing a specially crafted web page using Internet Explorer.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows XP x32 Service Pack 3 and prior
- Microsoft Windows XP x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
Flaw in the InformationCardSigninHelper Class ActiveX control (icardie.dll) and can be exploited to corrupt the system state.

Vulnerability Detection Method
Gets the ActiveX control (CLSID) information from the registry and checks if the appropriate patch has been applied.
Details: `Microsoft Windows ActiveX Control RCE Vulnerability (2900986)`
OID:1.3.6.1.4.1.25623.1.0.901225
Version used: `2023-09-22T16:08:59Z`

References

```
cve: CVE-2013-3918
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-090
url: http://www.securityfocus.com/bid/63631
url: http://www.zdnet.com/microsoft-to-patch-zero-day-bug-tuesday-7000023066/
url: http://www.fireeye.com/blog/uncategorized/2013/11/new-ie-zero-day-found-in-
↪watering-hole-attack.html
```

. . . continues on next page . . .

... continued from previous page ...

```
url: http://blogs.technet.com/b/msrc/archive/2013/11/11/activex-control-issue-be
↪ing-addressed-in-update-tuesday.aspx
cert-bund: CB-K13/0909
cert-bund: CB-K13/0905
dfn-cert: DFN-CERT-2013-1921
dfn-cert: DFN-CERT-2013-1920
```

High (CVSS: 9.3)
NVT: Microsoft Windows Kernel-Mode Drivers Code Execution Vulnerability (3119075)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-135.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\User32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19061
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code in kernel mode with elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
Multiple flaws are due to:
- Multiple local privilege-escalation vulnerabilities.
- Multiple remote code execution vulnerabilities when the Windows font library improperly handles specially crafted embedded fonts

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

... continues on next page ...

. . . continued from previous page . . .

Details: `Microsoft Windows Kernel-Mode Drivers Code Execution Vulnerability (3119075)`
OID:1.3.6.1.4.1.25623.1.0.806776
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-6171
cve: CVE-2015-6173
cve: CVE-2015-6174
cve: CVE-2015-6175
cve: CVE-2015-6106
cve: CVE-2015-6107
cve: CVE-2015-6108
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3119075
url: http://www.securityfocus.com/bid/78509
url: http://www.securityfocus.com/bid/78510
url: http://www.securityfocus.com/bid/78513
url: http://www.securityfocus.com/bid/78514
url: http://www.securityfocus.com/bid/78497
url: http://www.securityfocus.com/bid/78498
url: http://www.securityfocus.com/bid/78499
url: https://technet.microsoft.com/library/security/MS15-135
url: https://technet.microsoft.com/library/security/MS15-128
cert-bund: CB-K15/1804
dfn-cert: DFN-CERT-2015-1903
```

High (CVSS: 9.3)
NVT: Microsoft Windows Kernel-Mode Driver Privilege Escalation and RCE Vulnerabilities (3000061)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS14-058.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attacker to gain escalated privilege and compromise a user's system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2

Vulnerability Insight

The flaw is due to errors in win32k.sys when handling certain objects and parsing TrueType fonts.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel-Mode Driver Privilege Escalation and RCE Vulnerabiliti.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.804859

Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-4113
cve: CVE-2014-4148
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/3000061
url: http://www.securityfocus.com/bid/70364
url: http://www.securityfocus.com/bid/70429
url: https://technet.microsoft.com/library/security/ms14-058
cert-bund: CB-K14/1291
```

High (CVSS: 9.3)
NVT: Microsoft Windows IME (Japanese) Privilege Elevation Vulnerability (2992719)

Summary

This host is missing a moderate security update according to Microsoft Bulletin MS14-078.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attacker to bypass a sandbox protection mechanism via a crafted PDF document.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

Error in 'IMJPDCT.EXE', which allow remote attackers to bypass a sandbox protection mechanism via a crafted PDF document. Aka 'Microsoft IME (Japanese) Elevation of Privilege Vulnerability' as exploited in the wild in 2014.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows IME (Japanese) Privilege Elevation Vulnerability (2992719)`
OID:1.3.6.1.4.1.25623.1.0.802088
Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-4077
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/2991963
url: http://www.securityfocus.com/bid/70944
url: https://technet.microsoft.com/library/security/MS14-078
url: http://blogs.technet.com/b/srd/archive/2014/11/11/assessing-risk-for-the-no
↪vember-2014-security-updates.aspx
cert-bund: CB-K14/1402
cert-bund: CB-K14/1397
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3032359)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-018.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attackers to access information from one domain and inject it into another domain, execute arbitrary script with elevated privileges, corrupt memory and compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x and VBScript 5.8 on IE 8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to improper handling of cross-domain policies, improper validation of permissions under specific conditions and not properly handling objects in memory by VBScript engine, when rendered in Internet Explorer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3032359)`
OID:1.3.6.1.4.1.25623.1.0.805143
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0032
cve: CVE-2015-0056
cve: CVE-2015-0072
cve: CVE-2015-0099
cve: CVE-2015-0100
cve: CVE-2015-1622
cve: CVE-2015-1623
cve: CVE-2015-1624
cve: CVE-2015-1625
cve: CVE-2015-1626
cve: CVE-2015-1627
cve: CVE-2015-1634
url: https://support.microsoft.com/kb/3032359
url: http://www.securityfocus.com/bid/72489
url: https://technet.microsoft.com/en-us/library/security/ms15-018.aspx
cert-bund: CB-K15/0319
cert-bund: CB-K15/0318
dfn-cert: DFN-CERT-2015-0329
dfn-cert: DFN-CERT-2015-0324
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3034682)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-009.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow context
- dependent attacker to corrupt memory, execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 6.x/7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to an error related to display:run-in handling, user supplied input is not properly validated and multiple unspecified vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities (3034682)`
OID:1.3.6.1.4.1.25623.1.0.805136
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2014-8967
cve: CVE-2015-0017
cve: CVE-2015-0018
cve: CVE-2015-0019
cve: CVE-2015-0020
cve: CVE-2015-0021
cve: CVE-2015-0022
cve: CVE-2015-0023
cve: CVE-2015-0025
cve: CVE-2015-0026
cve: CVE-2015-0027
cve: CVE-2015-0028
cve: CVE-2015-0029
cve: CVE-2015-0030
cve: CVE-2015-0031
cve: CVE-2015-0035
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2015-0036
cve: CVE-2015-0037
cve: CVE-2015-0038
cve: CVE-2015-0039
cve: CVE-2015-0040
cve: CVE-2015-0041
cve: CVE-2015-0042
cve: CVE-2015-0043
cve: CVE-2015-0044
cve: CVE-2015-0045
cve: CVE-2015-0046
cve: CVE-2015-0048
cve: CVE-2015-0049
cve: CVE-2015-0050
cve: CVE-2015-0051
cve: CVE-2015-0052
cve: CVE-2015-0053
cve: CVE-2015-0054
cve: CVE-2015-0055
cve: CVE-2015-0066
cve: CVE-2015-0067
cve: CVE-2015-0068
cve: CVE-2015-0069
cve: CVE-2015-0070
cve: CVE-2015-0071
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/kb/3034682
url: http://www.securityfocus.com/bid/71483
url: http://www.securityfocus.com/bid/72402
url: http://www.securityfocus.com/bid/72403
url: http://www.securityfocus.com/bid/72425
url: http://www.securityfocus.com/bid/72426
url: http://www.securityfocus.com/bid/72436
url: http://www.securityfocus.com/bid/72437
url: http://www.securityfocus.com/bid/72438
url: http://www.securityfocus.com/bid/72439
url: http://www.securityfocus.com/bid/72440
url: http://www.securityfocus.com/bid/72441
url: http://www.securityfocus.com/bid/72442
url: http://www.securityfocus.com/bid/72443
url: http://www.securityfocus.com/bid/72444
url: http://www.securityfocus.com/bid/72445
url: http://www.securityfocus.com/bid/72447
url: http://www.securityfocus.com/bid/72446
url: http://www.securityfocus.com/bid/72448
url: http://www.securityfocus.com/bid/72404
```

... continues on next page ...

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/72409
url: http://www.securityfocus.com/bid/72410
url: http://www.securityfocus.com/bid/72411
url: http://www.securityfocus.com/bid/72412
url: http://www.securityfocus.com/bid/72413
url: http://www.securityfocus.com/bid/72414
url: http://www.securityfocus.com/bid/72415
url: http://www.securityfocus.com/bid/72416
url: http://www.securityfocus.com/bid/72417
url: http://www.securityfocus.com/bid/72418
url: http://www.securityfocus.com/bid/72419
url: http://www.securityfocus.com/bid/72453
url: http://www.securityfocus.com/bid/72420
url: http://www.securityfocus.com/bid/72421
url: http://www.securityfocus.com/bid/72478
url: http://www.securityfocus.com/bid/72479
url: http://www.securityfocus.com/bid/72422
url: http://www.securityfocus.com/bid/72423
url: http://www.securityfocus.com/bid/72424
url: http://www.securityfocus.com/bid/72454
url: http://www.securityfocus.com/bid/72480
url: http://www.securityfocus.com/bid/72455
url: https://technet.microsoft.com/library/security/MS15-009
cert-bund: CB-K15/0173
cert-bund: CB-K14/1535
dfn-cert: DFN-CERT-2015-0183
```

High (CVSS: 9.3)
NVT: Microsoft Windows Graphics Device Interface RCE Vulnerability (2876331)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS13-089.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to execute arbitrary code or cause a denial of service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight

Flaw is due to when Microsoft Windows improperly handles image in a Windows Write (.wri) document.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Graphics Device Interface RCE Vulnerability (2876331)`

OID:1.3.6.1.4.1.25623.1.0.903226

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-3940
url: http://support.microsoft.com/kb/2876331
url: http://www.securityfocus.com/bid/63546
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-089
cert-bund: CB-K13/0909
dfn-cert: DFN-CERT-2013-1921
```

High (CVSS: 9.0)

NVT: Microsoft Windows Print Spooler Components Privilege Escalation Vulnerability (2839894)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-050.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow remote attackers to execute arbitrary code with system privileges, resulting in complete compromise of the target.

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

The vulnerability is caused due to improper memory operations performed by the affected software when deleting printer connections.

Vulnerability Detection Method

Details: `Microsoft Windows Print Spooler Components Privilege Escalation Vulnerability (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.903212

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-1339
url: http://support.microsoft.com/kb/2839894
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-050
url: http://tools.cisco.com/security/center/viewAlert.x?alertId=29560
dfn-cert: DFN-CERT-2013-1113
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4480970)

Summary

This host is missing an important security update according to Microsoft KB4480970

Vulnerability Detection Result

```
Vulnerable range:   Less than 11.0.9600.19236
File checked:       C:\Windows\system32\Mshtml.dll
File version:       8.0.7601.17514
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code on a victim system, obtain information to further compromise the user's system and gain elevated privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flawss exists due to:
- Windows Jet Database Engine improperly handles objects in memory.
- Windows Runtime improperly handles objects in memory.
- Windows kernel improperly handles objects in memory.
- An error in the Microsoft XmlDocument class that could allow an attacker to escape from the AppContainer sandbox in the browser.
- MSHTML engine improperly validates input.
- Windows improperly handles authentication requests.
- An elevation of privilege exists in Windows COM Desktop Broker.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4480970)`
OID:1.3.6.1.4.1.25623.1.0.814650
Version used: `2023-10-27T16:11:32Z`

References
```
cve: CVE-2019-0536
cve: CVE-2019-0538
cve: CVE-2019-0541
cve: CVE-2019-0543
cve: CVE-2019-0584
cve: CVE-2019-0554
cve: CVE-2019-0549
cve: CVE-2019-0569
cve: CVE-2019-0583
cve: CVE-2019-0575
cve: CVE-2019-0576
cve: CVE-2019-0577
cve: CVE-2019-0578
cve: CVE-2019-0579
cve: CVE-2019-0580
cve: CVE-2019-0581
cve: CVE-2019-0582
cve: CVE-2018-3639
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4480963
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2072
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K19/0271
cert-bund: CB-K19/0047
cert-bund: CB-K19/0024
cert-bund: CB-K19/0023
cert-bund: CB-K19/0019
cert-bund: CB-K18/1050
cert-bund: CB-K18/0686
cert-bund: CB-K18/0682
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2020-1987
dfn-cert: DFN-CERT-2020-1935
dfn-cert: DFN-CERT-2020-1912
dfn-cert: DFN-CERT-2020-1783
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0286
dfn-cert: DFN-CERT-2019-0258
dfn-cert: DFN-CERT-2019-0168
dfn-cert: DFN-CERT-2019-0108
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2019-0047
dfn-cert: DFN-CERT-2019-0041
dfn-cert: DFN-CERT-2019-0039
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2302
dfn-cert: DFN-CERT-2018-2217
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1767
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1658
dfn-cert: DFN-CERT-2018-1651
dfn-cert: DFN-CERT-2018-1627
dfn-cert: DFN-CERT-2018-1624
dfn-cert: DFN-CERT-2018-1500
dfn-cert: DFN-CERT-2018-1494
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1493
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1374
dfn-cert: DFN-CERT-2018-1353
dfn-cert: DFN-CERT-2018-1351
dfn-cert: DFN-CERT-2018-1323
dfn-cert: DFN-CERT-2018-1304
dfn-cert: DFN-CERT-2018-1270
dfn-cert: DFN-CERT-2018-1260
dfn-cert: DFN-CERT-2018-1234
dfn-cert: DFN-CERT-2018-1228
dfn-cert: DFN-CERT-2018-1205
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-1151
dfn-cert: DFN-CERT-2018-1129
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1105
dfn-cert: DFN-CERT-2018-1042
dfn-cert: DFN-CERT-2018-1041
dfn-cert: DFN-CERT-2018-1025
dfn-cert: DFN-CERT-2018-1023
dfn-cert: DFN-CERT-2018-0993
dfn-cert: DFN-CERT-2018-0992
dfn-cert: DFN-CERT-2018-0991
dfn-cert: DFN-CERT-2018-0987
dfn-cert: DFN-CERT-2018-0976
dfn-cert: DFN-CERT-2018-0973
dfn-cert: DFN-CERT-2018-0972
dfn-cert: DFN-CERT-2018-0970
dfn-cert: DFN-CERT-2018-0966
```

High (CVSS: 8.8)
NVT: Microsoft Windows XML Core Services Remote Code Execution Vulnerability (3148541)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-040.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Msxml3.dll
File version:     8.110.7601.17514
Vulnerable range: Less than 8.110.7601.23373
```

Impact

Successful exploitation will allow remote attackers to run malicious code remotely to take control of the user's system.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Flaw exists due to some unspecified error when XML Core services parser processes user input.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows XML Core Services Remote Code Execution Vulnerability (314854.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.807539
Version used: `2023-07-20T05:05:17Z`

References
```
cve: CVE-2016-0147
url: https://support.microsoft.com/kb/3146963
url: https://technet.microsoft.com/library/security/MS16-040
url: https://technet.microsoft.com/library/security/MS15-040
cert-bund: CB-K16/0546
```

High (CVSS: 8.8)
NVT: Microsoft Windows Remote Privilege Escalation Vulnerability (3155520)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-061.

Vulnerability Detection Result
```
File checked:     C:\Windows\System32\Ntoskrnl.exe
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.23418
```

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow remote attackers to execute arbitrary code with elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
Flaw exists due to when windows improperly handles specially crafted Remote Procedure Call (RPC) requests.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Remote Privilege Escalation Vulnerability (3155520)`
OID:1.3.6.1.4.1.25623.1.0.807587
Version used: `2023-07-20T05:05:17Z`

References
```
cve: CVE-2016-0178
url: https://support.microsoft.com/kb/3153171
url: https://technet.microsoft.com/library/security/MS16-061
cert-bund: CB-K16/0701
```

High (CVSS: 8.8)
NVT: Microsoft Windows Print Spooler RCE Vulnerability (KB5005010, PrintNightmare)

Summary
This host is missing a critical security update according to Microsoft KB5005010. The flaw is dubbed 'PrintNightmare'.

Vulnerability Detection Result
```
Installed version: 6.1.7601.17514
Fixed version:     6.1.7601.25633
In order to secure your system, please also confirm that the following registry
↪keys are set to 0 (zero) or are not present:
```

... continues on next page ...

. . . continued from previous page . . .

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
 - NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)
 - UpdatePromptSettings = 0 (DWORD) or not defined (default setting)
```

Impact

Successful exploitation allow attackers to execute arbitrary code with SYSTEM privileges on a vulnerable system.

Solution:

Solution type: Workaround

The vendor has released updates.

In addition to installing the updates users are recommended to either disable the Print Spooler service, or to Disable inbound remote printing through Group Policy.

Please see the references for more information.

Affected Software/OS

- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows 7 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2008 x32
- Microsoft Windows Server 2008 R2 x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight

The flaw is due to the Microsoft Windows Print Spooler service which fails to restrict access to functionality that allows users to add printers and related drivers.

Vulnerability Detection Method

Check if a vulnerable file and registry configuration is present on the target host.

Details: `Microsoft Windows Print Spooler RCE Vulnerability (KB5005010, PrintNightmare)`

OID:1.3.6.1.4.1.25623.1.0.818162

Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2021-34527
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5005010
url: https://msrc-blog.microsoft.com/2021/07/08/clarified-guidance-for-cve-2021-
↪34527-windows-print-spooler-vulnerability/
cert-bund: CB-K21/0708
dfn-cert: DFN-CERT-2021-1437
```

High (CVSS: 8.8)
NVT: Microsoft Windows Netlogon Remote Code Execution Vulnerability (3167691)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-076.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\drivers\cng.sys
File version:     6.1.7601.18739
Vulnerable range: Less than 6.1.7601.23451
```

Impact
Successful exploitation will allow attackers to execute arbitrary code in the context of the currently logged-in user. Failed exploit attempts will likely result in denial of service conditions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1

Vulnerability Insight
The flaw occurs when windows improperly handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Netlogon Remote Code Execution Vulnerability (3167691)`
OID:1.3.6.1.4.1.25623.1.0.808227
Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-3228
url: https://support.microsoft.com/en-us/kb/3167691
url: https://technet.microsoft.com/library/security/MS16-076
cert-bund: CB-K16/0914
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5034831)

Summary
This host is missing an important security update according to Microsoft KB5034831

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable range:  Less than 6.1.7601.26958
File checked:      C:\Windows\system32\Conhost.exe
File version:      6.1.7601.17514
```

Impact

Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information, conduct spoofing and denial of service attacks on an affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1.

Vulnerability Insight

Multiple flaws exist due to,
- Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability.
- Windows Printing Service Spoofing Vulnerability.
- Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5034831)`
OID:1.3.6.1.4.1.25623.1.0.832825
Version used: `2024-02-15T05:05:40Z`

References

```
cve: CVE-2024-21420
cve: CVE-2024-21406
cve: CVE-2024-21375
cve: CVE-2024-21370
cve: CVE-2024-21368
cve: CVE-2024-21366
cve: CVE-2024-21365
cve: CVE-2024-21361
cve: CVE-2024-21360
cve: CVE-2024-21359
cve: CVE-2024-21358
cve: CVE-2024-21357
cve: CVE-2024-21356
cve: CVE-2024-21355
cve: CVE-2024-21354
cve: CVE-2024-21352
cve: CVE-2024-21350
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2024-21349
cve: CVE-2024-21347
cve: CVE-2024-21340
cve: CVE-2023-50387
cve: CVE-2024-21405
cve: CVE-2024-21391
cve: CVE-2024-21372
cve: CVE-2024-21369
cve: CVE-2024-21367
cve: CVE-2024-21363
url: https://support.microsoft.com/en-us/help/5034831
cert-bund: WID-SEC-2024-1313
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0387
cert-bund: WID-SEC-2024-0386
dfn-cert: DFN-CERT-2024-1516
dfn-cert: DFN-CERT-2024-1474
dfn-cert: DFN-CERT-2024-1223
dfn-cert: DFN-CERT-2024-0984
dfn-cert: DFN-CERT-2024-0977
dfn-cert: DFN-CERT-2024-0921
dfn-cert: DFN-CERT-2024-0829
dfn-cert: DFN-CERT-2024-0529
dfn-cert: DFN-CERT-2024-0498
dfn-cert: DFN-CERT-2024-0404
dfn-cert: DFN-CERT-2024-0399
dfn-cert: DFN-CERT-2024-0387
dfn-cert: DFN-CERT-2024-0379
dfn-cert: DFN-CERT-2024-0375
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5022338)

Summary
This host is missing an important security update according to Microsoft KB5022338

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.26321
File checked:      C:\Windows\system32\Ntoskrnl.exe
File version:      6.1.7601.18741
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- A Remote Code Execution Vulnerability in Windows Layer 2 Tunneling Protocol.
- An elevation of privilege vulnerability in Windows Kernel.
- A Denial of Service Vulnerability in Windows Layer 2 Tunneling Protocol.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5022338)`
OID:1.3.6.1.4.1.25623.1.0.826831
Version used: `2023-10-13T05:06:10Z`

References
```
cve: CVE-2023-21546
cve: CVE-2023-21543
cve: CVE-2023-21548
cve: CVE-2023-21555
cve: CVE-2023-21556
cve: CVE-2023-21561
cve: CVE-2023-21679
cve: CVE-2023-21730
cve: CVE-2023-21527
cve: CVE-2023-21532
cve: CVE-2023-21537
cve: CVE-2023-21541
cve: CVE-2023-21542
cve: CVE-2023-21549
cve: CVE-2023-21552
cve: CVE-2023-21557
cve: CVE-2023-21560
cve: CVE-2023-21563
cve: CVE-2023-21675
cve: CVE-2023-21678
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2023-21680
cve: CVE-2023-21681
cve: CVE-2023-21682
cve: CVE-2023-21726
cve: CVE-2023-21728
cve: CVE-2023-21732
cve: CVE-2023-21746
cve: CVE-2023-21748
cve: CVE-2023-21750
cve: CVE-2023-21757
cve: CVE-2023-21774
cve: CVE-2023-21525
cve: CVE-2023-21765
cve: CVE-2023-21752
cve: CVE-2023-21776
cve: CVE-2023-21749
cve: CVE-2023-21772
cve: CVE-2023-21524
cve: CVE-2023-21747
cve: CVE-2023-21773
cve: CVE-2023-21754
cve: CVE-2023-21760
url: https://support.microsoft.com/en-us/help/50122338
cert-bund: WID-SEC-2023-0055
dfn-cert: DFN-CERT-2023-0050
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5020000)

Summary
This host is missing a critical security update according to Microsoft KB5020000

Vulnerability Detection Result

```
Vulnerable range:   Less than 11.0.9600.20671
File checked:       C:\Windows\system32\urlmon.dll
File version:       8.0.7601.17514
```

Impact
Successful exploitation will allow an attacker to disclose sensitive information, perform remote code execution, cause denial of service condition and elevate privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:
- Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability.
- An elevation of privilege vulnerability in Windows Kerberos RC4-HMAC.
- Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5020000)`
OID:1.3.6.1.4.1.25623.1.0.826613
Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-23824
cve: CVE-2022-37966
cve: CVE-2022-37967
cve: CVE-2022-37992
cve: CVE-2022-38023
cve: CVE-2022-41039
cve: CVE-2022-41044
cve: CVE-2022-41045
cve: CVE-2022-41047
cve: CVE-2022-41048
cve: CVE-2022-41053
cve: CVE-2022-41056
cve: CVE-2022-41057
cve: CVE-2022-41058
cve: CVE-2022-41073
cve: CVE-2022-41086
cve: CVE-2022-41090
cve: CVE-2022-41095
cve: CVE-2022-41097
cve: CVE-2022-41098
cve: CVE-2022-41109
cve: CVE-2022-41116
cve: CVE-2022-41118
cve: CVE-2022-41128
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5020000
cert-bund: WID-SEC-2024-0064
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2022-2365
cert-bund: WID-SEC-2022-2001
cert-bund: WID-SEC-2022-1983
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-1311
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0665
dfn-cert: DFN-CERT-2023-0286
dfn-cert: DFN-CERT-2023-0201
dfn-cert: DFN-CERT-2023-0199
dfn-cert: DFN-CERT-2023-0176
dfn-cert: DFN-CERT-2023-0153
dfn-cert: DFN-CERT-2023-0089
dfn-cert: DFN-CERT-2022-2870
dfn-cert: DFN-CERT-2022-2526
dfn-cert: DFN-CERT-2022-2429
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5018454)

Summary
This host is missing an important security update according to Microsoft KB5018454

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.26174
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privilege, execute arbitrary code and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- A Remote Code Execution Vulnerability in Windows Point-to-Point Tunneling Protocol.

. . . continues on next page . . .

. . . continued from previous page . . .

- An elevation of privilege vulnerability in Active Directory Domain Services.
- A Denial of Service Vulnerability in Windows TCP/IP Driver.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5018454)`
OID:1.3.6.1.4.1.25623.1.0.826570
Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-22035
cve: CVE-2022-24504
cve: CVE-2022-30198
cve: CVE-2022-33634
cve: CVE-2022-33635
cve: CVE-2022-33645
cve: CVE-2022-35770
cve: CVE-2022-37975
cve: CVE-2022-37976
cve: CVE-2022-37977
cve: CVE-2022-37978
cve: CVE-2022-37981
cve: CVE-2022-37982
cve: CVE-2022-37985
cve: CVE-2022-37986
cve: CVE-2022-37987
cve: CVE-2022-37988
cve: CVE-2022-37989
cve: CVE-2022-37990
cve: CVE-2022-37991
cve: CVE-2022-37993
cve: CVE-2022-37994
cve: CVE-2022-37997
cve: CVE-2022-37999
cve: CVE-2022-38000
cve: CVE-2022-38022
cve: CVE-2022-38026
cve: CVE-2022-38029
cve: CVE-2022-38031
cve: CVE-2022-38032
cve: CVE-2022-38033
cve: CVE-2022-38034
cve: CVE-2022-38037
cve: CVE-2022-38038
cve: CVE-2022-38040
cve: CVE-2022-38041
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2022-38042
cve: CVE-2022-38043
cve: CVE-2022-38044
cve: CVE-2022-38047
cve: CVE-2022-38051
cve: CVE-2022-41033
cve: CVE-2022-41081
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5018454
cert-bund: WID-SEC-2022-1682
dfn-cert: DFN-CERT-2022-2249
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5015861)

Summary
This host is missing an important security update according to Microsoft KB5015861

Vulnerability Detection Result

```
Vulnerable range:   6.1.7601.0 - 6.1.7601.26021
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information, bypass security restrictions and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An elevation of privilege vulnerability in Windows Fax Service.
- A Remote Code Execution Vulnerability in Windows Graphics Component.
- A Denial of Service Vulnerability in Windows Security Account Manager.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5015861)`
OID:1.3.6.1.4.1.25623.1.0.821171
Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-21845
cve: CVE-2022-22022
cve: CVE-2022-22023
cve: CVE-2022-22024
cve: CVE-2022-22025
cve: CVE-2022-22026
cve: CVE-2022-22027
cve: CVE-2022-22028
cve: CVE-2022-22029
cve: CVE-2022-22034
cve: CVE-2022-22036
cve: CVE-2022-22037
cve: CVE-2022-22039
cve: CVE-2022-22040
cve: CVE-2022-22042
cve: CVE-2022-22043
cve: CVE-2022-22047
cve: CVE-2022-22048
cve: CVE-2022-22049
cve: CVE-2022-22050
cve: CVE-2022-30202
cve: CVE-2022-30203
cve: CVE-2022-30205
cve: CVE-2022-30206
cve: CVE-2022-30208
cve: CVE-2022-30209
cve: CVE-2022-30211
cve: CVE-2022-30213
cve: CVE-2022-30220
cve: CVE-2022-30221
cve: CVE-2022-30223
cve: CVE-2022-30224
cve: CVE-2022-30225
cve: CVE-2022-30226
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5015861
cert-bund: WID-SEC-2022-0649
dfn-cert: DFN-CERT-2022-1553
dfn-cert: DFN-CERT-2022-1293
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5014748)

Summary
This host is missing an important security update according to Microsoft KB5014748

Vulnerability Detection Result

```
Vulnerable range:  6.1.7601.0 - 6.1.7601.25982
File checked:      C:\Windows\system32\Ntoskrnl.exe
File version:      6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An elevation of privilege vulnerability in Local Security Authority Subsystem Service.
- A Remote Code Execution Vulnerability in Windows Hyper-V.
- A Denial of Service Vulnerability in Windows Kernel.

The flaw in the Microsoft Windows Support Diagnostic Tool (MSDT) and tracked via CVE-2022-30190 is dubbed 'Follina'.
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5014748)`
OID:1.3.6.1.4.1.25623.1.0.817782
Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-21123
cve: CVE-2022-21125
cve: CVE-2022-21127
cve: CVE-2022-21166
cve: CVE-2022-30135
cve: CVE-2022-30140
cve: CVE-2022-30141
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2022-30142
cve: CVE-2022-30143
cve: CVE-2022-30146
cve: CVE-2022-30147
cve: CVE-2022-30149
cve: CVE-2022-30151
cve: CVE-2022-30152
cve: CVE-2022-30153
cve: CVE-2022-30155
cve: CVE-2022-30160
cve: CVE-2022-30161
cve: CVE-2022-30163
cve: CVE-2022-30166
cve: CVE-2022-30190
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5014748
url: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190
url: https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-micr
↪osoft-support-diagnostic-tool-vulnerability/
url: https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerab
↪ility-1a47fce5629e
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-0336
cert-bund: WID-SEC-2022-0330
cert-bund: WID-SEC-2022-0325
cert-bund: WID-SEC-2022-0303
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2022-2858
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2446
dfn-cert: DFN-CERT-2022-2304
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1664
dfn-cert: DFN-CERT-2022-1663
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1636
dfn-cert: DFN-CERT-2022-1596
dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1529
dfn-cert: DFN-CERT-2022-1523
dfn-cert: DFN-CERT-2022-1519
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1413
dfn-cert: DFN-CERT-2022-1405
dfn-cert: DFN-CERT-2022-1378
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1365
dfn-cert: DFN-CERT-2022-1358
dfn-cert: DFN-CERT-2022-1345
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1342
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1338
dfn-cert: DFN-CERT-2022-1336
dfn-cert: DFN-CERT-2022-1334
dfn-cert: DFN-CERT-2022-1333
dfn-cert: DFN-CERT-2022-1328
dfn-cert: DFN-CERT-2022-1221
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5011552)

Summary
This host is missing an important security update according to Microsoft KB5011552

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.25895
File checked:      C:\Windows\system32\Ntoskrnl.exe
File version:      6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privileges, disclose sensitive information, conduct remote code execution, bypass security restrictions, and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to:

- An elevation of privilege vulnerability in Windows Fax and Scan Service.
- An elevation of privilege vulnerability in Windows ALPC.
- An elevation of privilege vulnerability in Windows Installer.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5011552)`

OID:1.3.6.1.4.1.25623.1.0.818979

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-21973
cve: CVE-2022-21990
cve: CVE-2022-23253
cve: CVE-2022-23281
cve: CVE-2022-23283
cve: CVE-2022-23285
cve: CVE-2022-23290
cve: CVE-2022-23293
cve: CVE-2022-23296
cve: CVE-2022-23297
cve: CVE-2022-23298
cve: CVE-2022-23299
cve: CVE-2022-24454
cve: CVE-2022-24459
cve: CVE-2022-24502
cve: CVE-2022-24503
url: https://support.microsoft.com/en-us/help/5011552
cert-bund: CB-K22/0290
dfn-cert: DFN-CERT-2022-0517
```

High (CVSS: 8.8)

NVT: Microsoft Windows Multiple Vulnerabilities (KB5009610)

Summary

This host is missing a critical security update according to Microsoft KB5009610

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.25827
File checked:       C:\Windows\system32\advapi32.dll
File version:       6.1.7600.16385
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow an attacker to elevate privileges, disclose sensitive information, conduct remote code execution, bypass security restrictions, conduct DoS attacks and conduct spoofing attacks.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- An elevation of privilege vulnerability in Active Directory Domain Services.
- An elevation of privilege vulnerability in Virtual Machine IDE Drive.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5009610)`

OID:1.3.6.1.4.1.25623.1.0.818952

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-21833
cve: CVE-2022-21834
cve: CVE-2022-21835
cve: CVE-2022-21836
cve: CVE-2022-21838
cve: CVE-2022-21843
cve: CVE-2022-21848
cve: CVE-2022-21850
cve: CVE-2022-21851
cve: CVE-2022-21857
cve: CVE-2022-21859
cve: CVE-2022-21862
cve: CVE-2022-21880
cve: CVE-2022-21883
cve: CVE-2022-21884
cve: CVE-2022-21885
cve: CVE-2022-21889
cve: CVE-2022-21890
cve: CVE-2022-21893
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2022-21897
cve: CVE-2022-21899
cve: CVE-2022-21900
cve: CVE-2022-21903
cve: CVE-2022-21904
cve: CVE-2022-21905
cve: CVE-2022-21908
cve: CVE-2022-21913
cve: CVE-2022-21914
cve: CVE-2022-21915
cve: CVE-2022-21916
cve: CVE-2022-21919
cve: CVE-2022-21920
cve: CVE-2022-21922
cve: CVE-2022-21924
cve: CVE-2022-21925
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5009610
cert-bund: WID-SEC-2023-0839
cert-bund: CB-K22/0030
dfn-cert: DFN-CERT-2022-0052
```

High (CVSS: 8.8)
NVT: Microsoft .NET Framework Multiple Vulnerabilities (KB4507420)

Summary
This host is missing a critical security update according to Microsoft KB4507420

Vulnerability Detection Result

```
Vulnerable range:  4.0.30319.30000 - 4.0.30319.36565
File checked:      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.identi
↪tymodel.dll
File version:      4.0.30319.34209
```

Impact
Successful exploitation will allow an attacker to gain elevated privileges, conduct denial-of-service condition and execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 and 4.8 on Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight

Multiple flaws exist due to:

- An error in Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF), allowing signing of SAML tokens with arbitrary symmetric keys.
- An error when Microsoft Common Object Runtime Library improperly handles web requests.
- Because the .NET Framework fails to check the source markup of a file.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Multiple Vulnerabilities (KB4507420)`

OID:1.3.6.1.4.1.25623.1.0.815156

Version used: `2022-04-13T07:21:45Z`

References

```
cve: CVE-2019-1113
cve: CVE-2019-1006
cve: CVE-2019-1083
url: https://support.microsoft.com/en-us/help/4506994/
url: http://www.securityfocus.com/bid/108977
url: http://www.securityfocus.com/bid/108978
url: http://www.securityfocus.com/bid/108981
url: https://support.microsoft.com/en-us/help/4506997/
url: https://support.microsoft.com/en-us/help/4507001/
url: https://support.microsoft.com/en-us/help/4507004/
url: https://support.microsoft.com/en-us/help/4507420/
cert-bund: CB-K19/0593
dfn-cert: DFN-CERT-2019-1397
dfn-cert: DFN-CERT-2019-1396
dfn-cert: DFN-CERT-2019-1392
dfn-cert: DFN-CERT-2019-1391
```

High (CVSS: 8.8)

NVT: Microsoft .NET Framework Multiple Vulnerabilities (KB4556399)

Summary

This host is missing a critical security update according to Microsoft KB4556399

Vulnerability Detection Result

```
Vulnerable range:   4.0 - 4.0.30319.36626
File checked:       C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.identi
↪tymodel.dll
File version:       4.0.30319.34209
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow an attacker to gain escalated privileges, conduct a denial-of-service condition and run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight

Multiple flaws exist due to:

- Microsoft .NET Framework fails to check the source markup of a file.
- Microsoft .NET Framework improperly handles web requests.
- An error in how .NET Framework activates COM objects.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Multiple Vulnerabilities (KB4556399)`

OID:1.3.6.1.4.1.25623.1.0.817103

Version used: `2021-08-11T12:01:46Z`

References

```
cve: CVE-2020-1108
cve: CVE-2020-0605
cve: CVE-2020-1066
url: https://support.microsoft.com/en-us/help/4556399/kb4556399
cert-bund: CB-K20/0456
cert-bund: CB-K20/0048
dfn-cert: DFN-CERT-2020-1091
dfn-cert: DFN-CERT-2020-1032
dfn-cert: DFN-CERT-2020-1009
dfn-cert: DFN-CERT-2020-1008
dfn-cert: DFN-CERT-2020-0087
```

High (CVSS: 8.8)

NVT: Microsoft Windows Multiple Vulnerabilities (KB5007236)

Summary

This host is missing a critical security update according to Microsoft KB5007236

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable range:  Less than 6.1.7601.25767
File checked:      C:\Windows\system32\advapi32.dll
File version:      6.1.7600.16385
```

Impact

Successful exploitation will allow an attacker to disclose sensitive information, perform remote code execution and elevate privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- An elevation of privilege vulnerability in Active Directory Domain Services.
- An elevation of privilege vulnerability in NTFS.
- An information disclosure vulnerability in Windows Remote Desktop Protocol (RDP).

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5007236)`

OID:1.3.6.1.4.1.25623.1.0.818854

Version used: `2024-01-01T05:05:52Z`

References

```
cve: CVE-2021-38631
cve: CVE-2021-38665
cve: CVE-2021-38666
cve: CVE-2021-41367
cve: CVE-2021-41370
cve: CVE-2021-41371
cve: CVE-2021-41377
cve: CVE-2021-41379
cve: CVE-2021-42275
cve: CVE-2021-42278
cve: CVE-2021-42282
cve: CVE-2021-42283
cve: CVE-2021-42285
cve: CVE-2021-42287
cve: CVE-2021-42291
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5007236
cert-bund: CB-K21/1226
cert-bund: CB-K21/1169
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5006743)

Summary
This host is missing a critical security update according to Microsoft KB5006743

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.25740
File checked:      C:\Windows\system32\advapi32.dll
File version:      6.1.7600.16385
```

Impact
Successful exploitation will allow an attacker to disclose sensitive information, perform remote code execution, cause denial of service condition, conduct spoofing and elevate privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An error in Windows exFAT File System.
- An error in Windows Fast FAT File System Driver.
- A error in Windows Remote Procedure Call Runtime.
- An error in Windows Media Audio Decoder.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5006743)`
OID:1.3.6.1.4.1.25623.1.0.818808
Version used: `2023-10-20T16:09:12Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2021-26442
cve: CVE-2021-36953
cve: CVE-2021-36970
cve: CVE-2021-38662
cve: CVE-2021-38663
cve: CVE-2021-40443
cve: CVE-2021-40449
cve: CVE-2021-40455
cve: CVE-2021-40460
cve: CVE-2021-40465
cve: CVE-2021-40466
cve: CVE-2021-40467
cve: CVE-2021-40469
cve: CVE-2021-40489
cve: CVE-2021-41331
cve: CVE-2021-41332
cve: CVE-2021-41335
cve: CVE-2021-41340
cve: CVE-2021-41342
cve: CVE-2021-41343
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5006743
cert-bund: CB-K21/1068
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5005633)

Summary
This host is missing a critical security update according to Microsoft KB5005633

Vulnerability Detection Result

```
Vulnerable range:  Less than 11.0.9600.20120
File checked:      C:\Windows\system32\urlmon.dll
File version:      8.0.7601.17514
```

Impact
Successful exploitation will allow an attacker to disclose sensitive information, perform remote code execution, cause denial of service condition, conduct spoofing and elevate privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- An error in Windows Ancillary Function Driver for WinSock.
- An elevation of privilege vulnerability in Windows Event Tracing.
- A error in Microsoft MSHTML.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5005633)`

OID:1.3.6.1.4.1.25623.1.0.818533

Version used: `2024-01-01T05:05:52Z`

References

```
cve: CVE-2021-26435
cve: CVE-2021-36955
cve: CVE-2021-36959
cve: CVE-2021-36960
cve: CVE-2021-36961
cve: CVE-2021-36962
cve: CVE-2021-36963
cve: CVE-2021-36964
cve: CVE-2021-36965
cve: CVE-2021-36968
cve: CVE-2021-36969
cve: CVE-2021-38628
cve: CVE-2021-38629
cve: CVE-2021-38630
cve: CVE-2021-38633
cve: CVE-2021-38635
cve: CVE-2021-38636
cve: CVE-2021-38638
cve: CVE-2021-38639
cve: CVE-2021-38667
cve: CVE-2021-38671
cve: CVE-2021-40444
cve: CVE-2021-40447
cve: CVE-2021-36958
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5005633
cert-bund: CB-K21/0965
cert-bund: CB-K21/0940
```

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K21/0867
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5004289)

Summary
This host is missing a critical security update according to Microsoft KB5004289

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.25661
File checked:       C:\Windows\system32\advapi32.dll
File version:       6.1.7600.16385
```

Impact
Successful exploitation will allow an attacker to perform remote code execution, gain access to potentially sensitive data, conduct spoofing and elevate privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An elevation of privilege vulnerability in Windows Common Log File System Driver.
- A security feature bypass vulnerability in Kerberos AppContainer.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB5004289)`
OID:1.3.6.1.4.1.25623.1.0.817724
Version used: `2024-01-01T05:05:52Z`

References

```
cve: CVE-2021-31183
cve: CVE-2021-31979
cve: CVE-2021-33745
cve: CVE-2021-33746
cve: CVE-2021-33749
cve: CVE-2021-33750
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2021-33752
cve: CVE-2021-33754
cve: CVE-2021-33756
cve: CVE-2021-33757
cve: CVE-2021-33764
cve: CVE-2021-33765
cve: CVE-2021-33780
cve: CVE-2021-33782
cve: CVE-2021-33783
cve: CVE-2021-33786
cve: CVE-2021-33788
cve: CVE-2021-34440
cve: CVE-2021-34441
cve: CVE-2021-34442
cve: CVE-2021-34444
cve: CVE-2021-34446
cve: CVE-2021-34447
cve: CVE-2021-34448
cve: CVE-2021-34456
cve: CVE-2021-34457
cve: CVE-2021-34476
cve: CVE-2021-34492
cve: CVE-2021-34494
cve: CVE-2021-34496
cve: CVE-2021-34497
cve: CVE-2021-34498
cve: CVE-2021-34499
cve: CVE-2021-34500
cve: CVE-2021-34504
cve: CVE-2021-34507
cve: CVE-2021-34511
cve: CVE-2021-34514
cve: CVE-2021-34516
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5004289
cert-bund: CB-K21/0736
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5001335)

Summary
This host is missing a critical security update according to Microsoft KB5001335

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24576
```

. . . continues on next page . . .

... continued from previous page ...

```
File checked:      C:\Windows\system32\inetcomm.dll
File version:      6.1.7601.17514
```

Impact

Successful exploitation will allow an attacker to perform remote code execution, conduct a denial-of-service condition, gain access to potentially sensitive data, bypass security restrictions, conduct spoofing and elevate privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- Multiple errors in Windows Installer.
- An error in RPC Endpoint Mapper Service.
- An error in Microsoft Internet Messaging API.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5001335)`

OID:1.3.6.1.4.1.25623.1.0.817693

Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2021-26413
cve: CVE-2021-26415
cve: CVE-2021-27089
cve: CVE-2021-27091
cve: CVE-2021-27093
cve: CVE-2021-27095
cve: CVE-2021-27096
cve: CVE-2021-28309
cve: CVE-2021-28315
cve: CVE-2021-28316
cve: CVE-2021-28317
cve: CVE-2021-28318
cve: CVE-2021-28323
cve: CVE-2021-28327
cve: CVE-2021-28328
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2021-28329
cve: CVE-2021-28330
cve: CVE-2021-28331
cve: CVE-2021-28332
cve: CVE-2021-28333
cve: CVE-2021-28334
cve: CVE-2021-28335
cve: CVE-2021-28336
cve: CVE-2021-28337
cve: CVE-2021-28338
cve: CVE-2021-28339
cve: CVE-2021-28340
cve: CVE-2021-28341
cve: CVE-2021-28342
cve: CVE-2021-28343
cve: CVE-2021-28344
cve: CVE-2021-28345
cve: CVE-2021-28346
cve: CVE-2021-28348
cve: CVE-2021-28349
cve: CVE-2021-28350
cve: CVE-2021-28352
cve: CVE-2021-28353
cve: CVE-2021-28354
cve: CVE-2021-28355
cve: CVE-2021-28356
cve: CVE-2021-28357
cve: CVE-2021-28358
cve: CVE-2021-28434
cve: CVE-2021-28437
cve: CVE-2021-28439
cve: CVE-2021-28440
cve: CVE-2021-28443
cve: CVE-2021-28445
cve: CVE-2021-28446
url: https://support.microsoft.com/en-us/help/5001335
cert-bund: CB-K21/0374
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4598279)

Summary
This host is missing a critical security update according to Microsoft KB4598279

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24564
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
File checked:      C:\Windows\system32\Kernel32.dll
File version:      6.1.7601.17514
```

Impact

Successful exploitation will allow an attacker to perform remote code execution and elevate privilege.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- An error in Active Template Library.
- An error in Windows CSC Service.
- An error in TPM Device Driver.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4598279)`

OID:1.3.6.1.4.1.25623.1.0.817574

Version used: `2024-01-03T05:05:19Z`

References

```
cve: CVE-2021-1649
cve: CVE-2021-1652
cve: CVE-2021-1653
cve: CVE-2021-1654
cve: CVE-2021-1655
cve: CVE-2021-1656
cve: CVE-2021-1657
cve: CVE-2021-1658
cve: CVE-2021-1659
cve: CVE-2021-1660
cve: CVE-2021-1661
cve: CVE-2021-1664
cve: CVE-2021-1665
cve: CVE-2021-1666
cve: CVE-2021-1667
cve: CVE-2021-1668
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2021-1671
cve: CVE-2021-1673
cve: CVE-2021-1674
cve: CVE-2021-1676
cve: CVE-2021-1678
cve: CVE-2021-1679
cve: CVE-2021-1688
cve: CVE-2021-1693
cve: CVE-2021-1694
cve: CVE-2021-1695
cve: CVE-2021-1696
cve: CVE-2021-1699
cve: CVE-2021-1700
cve: CVE-2021-1701
cve: CVE-2021-1702
cve: CVE-2021-1704
cve: CVE-2021-1706
cve: CVE-2021-1708
cve: CVE-2021-1709
url: https://support.microsoft.com/en-us/help/4598279
cert-bund: CB-K21/0028
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4580345)

Summary
This host is missing a critical security update according to Microsoft KB4580345

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24561
File checked:      C:\Windows\system32\Conhost.exe
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code, elevate privileges and disclose sensitive information.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to:

- An error when the Windows Network Connections Service handles objects in memory.

- An error when the Windows KernelStream fails to properly handles objects in memory.

- An error when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system.

- An error when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory.

- An error when the Windows Event System improperly handles objects in memory.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4580345)`

OID:1.3.6.1.4.1.25623.1.0.817511

Version used: `2024-06-26T05:05:39Z`

References

```
cve: CVE-2020-16863
cve: CVE-2020-16887
cve: CVE-2020-16889
cve: CVE-2020-16891
cve: CVE-2020-16897
cve: CVE-2020-16900
cve: CVE-2020-16902
cve: CVE-2020-16912
cve: CVE-2020-16914
cve: CVE-2020-16916
cve: CVE-2020-16920
cve: CVE-2020-16922
cve: CVE-2020-16923
cve: CVE-2020-16924
cve: CVE-2020-16935
cve: CVE-2020-16936
cve: CVE-2020-16939
cve: CVE-2020-16940
cve: CVE-2020-16972
cve: CVE-2020-16973
cve: CVE-2020-16974
cve: CVE-2020-16975
cve: CVE-2020-16976
url: https://support.microsoft.com/en-us/help/4580345
cert-bund: CB-K20/0979
dfn-cert: DFN-CERT-2020-2244
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4577051)

Summary
This host is missing a critical security update according to Microsoft KB4577051

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24560
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code, elevate privileges, conduct DoS condition and disclose sensitive information.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to errors,
- when the Windows RSoP Service Application improperly handles memory.
- when Active Directory integrated DNS (ADIDNS) mishandles objects in memory.
- in how splwow64.exe handles certain calls.
- in the way that Microsoft COM for Windows handles objects in memory.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4577051)`
OID:1.3.6.1.4.1.25623.1.0.817365
Version used: `2024-06-26T05:05:39Z`

References
```
cve: CVE-2020-0648
cve: CVE-2020-0664
cve: CVE-2020-0718
cve: CVE-2020-0761
cve: CVE-2020-0782
cve: CVE-2020-0790
cve: CVE-2020-0836
cve: CVE-2020-0838
cve: CVE-2020-0856
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-0878
cve: CVE-2020-0911
cve: CVE-2020-0912
cve: CVE-2020-0921
cve: CVE-2020-0922
cve: CVE-2020-1012
cve: CVE-2020-1013
cve: CVE-2020-1030
cve: CVE-2020-1031
cve: CVE-2020-1038
cve: CVE-2020-1039
cve: CVE-2020-1052
cve: CVE-2020-1074
cve: CVE-2020-1083
cve: CVE-2020-1091
cve: CVE-2020-1097
cve: CVE-2020-1115
cve: CVE-2020-1228
cve: CVE-2020-1245
cve: CVE-2020-1250
cve: CVE-2020-1252
cve: CVE-2020-1256
cve: CVE-2020-1285
cve: CVE-2020-1376
cve: CVE-2020-1491
cve: CVE-2020-1508
cve: CVE-2020-1559
cve: CVE-2020-1589
cve: CVE-2020-1593
cve: CVE-2020-1596
cve: CVE-2020-1598
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4577051
cert-bund: CB-K20/0882
cert-bund: CB-K20/0880
cert-bund: CB-K20/0876
dfn-cert: DFN-CERT-2020-1955
dfn-cert: DFN-CERT-2020-1954
dfn-cert: DFN-CERT-2020-1953
dfn-cert: DFN-CERT-2020-1948
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4561643)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing a critical security update according to Microsoft KB4561643

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24556
File checked:      C:\Windows\system32\Kernel32.dll
File version:      6.1.7601.17514
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code, elevate privileges, disclose sensitive information, conduct spoofing and denial of service attacks.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- Multiple errors in Windows when the Windows kernel-mode driver fails to properly handle objects in memory.
- An error when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content.
- An error when Windows Modules Installer Service improperly handles class object members.
- An error in the way that the VBScript engine handles objects in memory.
- An error when the Windows kernel fails to properly handle objects in memory.
- An error in the way Windows Error Reporting (WER) handles objects in memory. Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4561643)`

OID:1.3.6.1.4.1.25623.1.0.817158

Version used: `2024-06-26T05:05:39Z`

References

```
cve: CVE-2020-1160
cve: CVE-2020-1194
cve: CVE-2020-1196
cve: CVE-2020-1207
cve: CVE-2020-1208
cve: CVE-2020-1212
cve: CVE-2020-1213
cve: CVE-2020-1214
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-1215
cve: CVE-2020-1216
cve: CVE-2020-1219
cve: CVE-2020-1220
cve: CVE-2020-1230
cve: CVE-2020-1236
cve: CVE-2020-1239
cve: CVE-2020-1246
cve: CVE-2020-1247
cve: CVE-2020-1251
cve: CVE-2020-1253
cve: CVE-2020-1254
cve: CVE-2020-1255
cve: CVE-2020-1260
cve: CVE-2020-1262
cve: CVE-2020-1263
cve: CVE-2020-1270
cve: CVE-2020-1271
cve: CVE-2020-1272
cve: CVE-2020-1281
cve: CVE-2020-1287
cve: CVE-2020-1291
cve: CVE-2020-1299
cve: CVE-2020-1300
cve: CVE-2020-1301
cve: CVE-2020-1302
cve: CVE-2020-1311
cve: CVE-2020-1314
cve: CVE-2020-1315
cve: CVE-2020-1317
cve: CVE-2020-1348
url: https://support.microsoft.com/en-us/help/4561643
cert-bund: CB-K20/0568
cert-bund: CB-K20/0565
cert-bund: CB-K20/0561
dfn-cert: DFN-CERT-2020-1227
dfn-cert: DFN-CERT-2020-1226
dfn-cert: DFN-CERT-2020-1225
dfn-cert: DFN-CERT-2020-1224
dfn-cert: DFN-CERT-2020-1223
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4550964)

Summary

This host is missing a critical security update according to Microsoft KB4550964

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24551
File checked:      C:\Windows\system32\Win32k.sys
File version:      6.1.7601.17514
```

Impact

Successful exploitation allows an attacker to execute arbitrary code on a victim system, disclose sensitive information, conduct denial-of-service condition and gain elevated privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to

- An error when the Windows kernel improperly handles objects in memory.
- Multiple errors in the way Microsoft Graphics Components handle objects in memory.
- Multiple errors when the Windows Jet Database Engine improperly handles objects in memory.
- An error in Windows DNS when it fails to properly handle queries.

Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4550964)`

OID:1.3.6.1.4.1.25623.1.0.816823

Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2020-0687
cve: CVE-2020-0821
cve: CVE-2020-0889
cve: CVE-2020-0895
cve: CVE-2020-0938
cve: CVE-2020-0946
cve: CVE-2020-0952
cve: CVE-2020-0953
cve: CVE-2020-0955
cve: CVE-2020-0956
cve: CVE-2020-0957
cve: CVE-2020-0958
cve: CVE-2020-0959
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-0960
cve: CVE-2020-0962
cve: CVE-2020-0964
cve: CVE-2020-0965
cve: CVE-2020-0966
cve: CVE-2020-0967
cve: CVE-2020-0968
cve: CVE-2020-0982
cve: CVE-2020-0987
cve: CVE-2020-0988
cve: CVE-2020-0992
cve: CVE-2020-0993
cve: CVE-2020-0994
cve: CVE-2020-0995
cve: CVE-2020-0999
cve: CVE-2020-1000
cve: CVE-2020-1004
cve: CVE-2020-1005
cve: CVE-2020-1007
cve: CVE-2020-1008
cve: CVE-2020-1009
cve: CVE-2020-1011
cve: CVE-2020-1014
cve: CVE-2020-1015
cve: CVE-2020-1020
cve: CVE-2020-1027
cve: CVE-2020-1094
cve: CVE-2020-0907
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4550964
cert-bund: CB-K20/0334
cert-bund: CB-K20/0332
cert-bund: CB-K20/0257
dfn-cert: DFN-CERT-2020-0761
dfn-cert: DFN-CERT-2020-0756
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4540688)

Summary
This host is missing a critical security update according to Microsoft KB4540688

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24550
File checked:       C:\Windows\system32\User32.dll
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
File version:      6.1.7601.17514
```

Impact

Successful exploitation allows an attacker to execute arbitrary code, elevate privileges, disclose sensitive information and conduct tampering attacks.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist when,
- Windows Error Reporting improperly handles memory.
- Windows GDI component improperly discloses the contents of its memory.
- Windows Graphics Component improperly handles objects in memory.
- Windows Network Connections Service improperly handles objects in memory.
- Connected User Experiences and Telemetry Service improperly handles file operations.

Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4540688)`
OID:1.3.6.1.4.1.25623.1.0.815797
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2020-0645
cve: CVE-2020-0684
cve: CVE-2020-0768
cve: CVE-2020-0769
cve: CVE-2020-0770
cve: CVE-2020-0771
cve: CVE-2020-0772
cve: CVE-2020-0773
cve: CVE-2020-0774
cve: CVE-2020-0778
cve: CVE-2020-0779
cve: CVE-2020-0781
cve: CVE-2020-0783
cve: CVE-2020-0785
cve: CVE-2020-0787
cve: CVE-2020-0788
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-0791
cve: CVE-2020-0802
cve: CVE-2020-0803
cve: CVE-2020-0804
cve: CVE-2020-0806
cve: CVE-2020-0814
cve: CVE-2020-0822
cve: CVE-2020-0824
cve: CVE-2020-0830
cve: CVE-2020-0832
cve: CVE-2020-0833
cve: CVE-2020-0842
cve: CVE-2020-0843
cve: CVE-2020-0844
cve: CVE-2020-0845
cve: CVE-2020-0847
cve: CVE-2020-0849
cve: CVE-2020-0853
cve: CVE-2020-0860
cve: CVE-2020-0871
cve: CVE-2020-0874
cve: CVE-2020-0877
cve: CVE-2020-0879
cve: CVE-2020-0880
cve: CVE-2020-0881
cve: CVE-2020-0882
cve: CVE-2020-0883
cve: CVE-2020-0885
cve: CVE-2020-0887
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4540688
cert-bund: WID-SEC-2022-0289
cert-bund: CB-K20/0212
cert-bund: CB-K20/0210
cert-bund: CB-K20/0209
dfn-cert: DFN-CERT-2020-0500
dfn-cert: DFN-CERT-2020-0494
dfn-cert: DFN-CERT-2020-0493
dfn-cert: DFN-CERT-2020-0492
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4537820)

Summary
This host is missing a critical security update according to Microsoft KB4537820

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24548
File checked:      C:\Windows\system32\Win32k.sys
File version:      6.1.7601.17514
```

Impact

Successful exploitation will allow an attacker to run arbitrary code, elevate privileges and disclose sensitive information

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to

- Windows Common Log File System (CLFS) driver fails to properly handle objects in memory.
- Windows Search Indexer improperly handles objects in memory.
- Cryptography Next Generation (CNG) service improperly handles objects in memory.
- Windows Error Reporting manager improperly handles hard links.
- Windows Function Discovery Service improperly handles objects in memory.

Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4537820)`

OID:1.3.6.1.4.1.25623.1.0.815776

Version used: `2024-06-26T05:05:39Z`

References

```
cve: CVE-2020-0655
cve: CVE-2020-0657
cve: CVE-2020-0658
cve: CVE-2020-0662
cve: CVE-2020-0665
cve: CVE-2020-0666
cve: CVE-2020-0667
cve: CVE-2020-0668
cve: CVE-2020-0673
cve: CVE-2020-0674
cve: CVE-2020-0675
cve: CVE-2020-0676
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-0677
cve: CVE-2020-0678
cve: CVE-2020-0680
cve: CVE-2020-0681
cve: CVE-2020-0682
cve: CVE-2020-0683
cve: CVE-2020-0686
cve: CVE-2020-0691
cve: CVE-2020-0698
cve: CVE-2020-0703
cve: CVE-2020-0705
cve: CVE-2020-0708
cve: CVE-2020-0715
cve: CVE-2020-0719
cve: CVE-2020-0720
cve: CVE-2020-0721
cve: CVE-2020-0722
cve: CVE-2020-0723
cve: CVE-2020-0724
cve: CVE-2020-0725
cve: CVE-2020-0726
cve: CVE-2020-0729
cve: CVE-2020-0730
cve: CVE-2020-0731
cve: CVE-2020-0734
cve: CVE-2020-0735
cve: CVE-2020-0736
cve: CVE-2020-0737
cve: CVE-2020-0738
cve: CVE-2020-0744
cve: CVE-2020-0745
cve: CVE-2020-0748
cve: CVE-2020-0752
cve: CVE-2020-0753
cve: CVE-2020-0754
cve: CVE-2020-0755
cve: CVE-2020-0756
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4537820
cert-bund: WID-SEC-2022-2120
cert-bund: CB-K20/0123
cert-bund: CB-K20/0114
cert-bund: CB-K20/0059
dfn-cert: DFN-CERT-2020-0306
dfn-cert: DFN-CERT-2020-0299
dfn-cert: DFN-CERT-2020-0133
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4530734)

Summary
This host is missing a critical security update according to Microsoft KB4530734

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24540
File checked:      C:\Windows\system32\Ntdll.dll
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code, elevate privileges, gain access to sensitive information, cause denial of service and bypass security restrictions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- Win32k component fails to properly handle objects in memory.
- win32k component improperly provides kernel information.
- Windows kernel improperly handles objects in memory.
- Windows improperly handles COM object creation.
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4530734)`
OID:1.3.6.1.4.1.25623.1.0.815737
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2019-1453
cve: CVE-2019-1458
cve: CVE-2019-1465
cve: CVE-2019-1466
cve: CVE-2019-1467
cve: CVE-2019-1468
cve: CVE-2019-1469
cve: CVE-2019-1470
cve: CVE-2019-1474
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2019-1478
cve: CVE-2019-1480
cve: CVE-2019-1481
cve: CVE-2019-1484
cve: CVE-2019-1485
cve: CVE-2019-1488
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4530734/
cert-bund: CB-K19/1075
cert-bund: CB-K19/1063
dfn-cert: DFN-CERT-2019-2603
dfn-cert: DFN-CERT-2019-2601
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4516065)

Summary
This host is missing a critical security update according to Microsoft KB4516065

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24520
File checked:      C:\Windows\system32\Advapi32.dll
File version:      6.1.7600.16385
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code on a victim system, obtain information to further compromise the user's system, gain elevated privileges and disclose sensitive information.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- Windows Remote Desktop Client improperly handles connection requests.
- VBScript engine improperly handles objects in memory.
- Windows Common Log File System (CLFS) driver improperly handles objects in memory.
- ws2ifsl.sys (Winsock) improperly handles objects in memory.
- DirectX improperly handles objects in memory.

. . . continues on next page . . .

. . . continued from previous page . . .

Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4516065)`

OID:1.3.6.1.4.1.25623.1.0.815462

Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2018-12126
cve: CVE-2018-12127
cve: CVE-2018-12130
cve: CVE-2019-0787
cve: CVE-2019-11091
cve: CVE-2019-1208
cve: CVE-2019-1214
cve: CVE-2019-1215
cve: CVE-2019-1216
cve: CVE-2019-1219
cve: CVE-2019-1220
cve: CVE-2019-1221
cve: CVE-2019-1235
cve: CVE-2019-1236
cve: CVE-2019-1240
cve: CVE-2019-1241
cve: CVE-2019-1242
cve: CVE-2019-1243
cve: CVE-2019-1244
cve: CVE-2019-1245
cve: CVE-2019-1246
cve: CVE-2019-1247
cve: CVE-2019-1248
cve: CVE-2019-1249
cve: CVE-2019-1250
cve: CVE-2019-1252
cve: CVE-2019-1256
cve: CVE-2019-1267
cve: CVE-2019-1268
cve: CVE-2019-1271
cve: CVE-2019-1274
cve: CVE-2019-1280
cve: CVE-2019-1282
cve: CVE-2019-1283
cve: CVE-2019-1284
cve: CVE-2019-1285
cve: CVE-2019-1286
cve: CVE-2019-1290
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2019-1291
cve: CVE-2019-1293
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4516065
cert-bund: WID-SEC-2023-1692
cert-bund: CB-K19/0811
cert-bund: CB-K19/0806
cert-bund: CB-K19/0804
cert-bund: CB-K19/0803
cert-bund: CB-K19/0414
dfn-cert: DFN-CERT-2020-1041
dfn-cert: DFN-CERT-2020-0069
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-2214
dfn-cert: DFN-CERT-2019-1985
dfn-cert: DFN-CERT-2019-1898
dfn-cert: DFN-CERT-2019-1893
dfn-cert: DFN-CERT-2019-1889
dfn-cert: DFN-CERT-2019-1886
dfn-cert: DFN-CERT-2019-1767
dfn-cert: DFN-CERT-2019-1414
dfn-cert: DFN-CERT-2019-1235
dfn-cert: DFN-CERT-2019-1200
dfn-cert: DFN-CERT-2019-1172
dfn-cert: DFN-CERT-2019-1151
dfn-cert: DFN-CERT-2019-1149
dfn-cert: DFN-CERT-2019-1122
dfn-cert: DFN-CERT-2019-1083
dfn-cert: DFN-CERT-2019-1036
dfn-cert: DFN-CERT-2019-1032
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-1025
dfn-cert: DFN-CERT-2019-1024
dfn-cert: DFN-CERT-2019-1017
dfn-cert: DFN-CERT-2019-1012
dfn-cert: DFN-CERT-2019-1009
dfn-cert: DFN-CERT-2019-1005
dfn-cert: DFN-CERT-2019-1004
dfn-cert: DFN-CERT-2019-1003
dfn-cert: DFN-CERT-2019-1002
dfn-cert: DFN-CERT-2019-0994
dfn-cert: DFN-CERT-2019-0990
dfn-cert: DFN-CERT-2019-0989
dfn-cert: DFN-CERT-2019-0988
dfn-cert: DFN-CERT-2019-0987
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-0986
dfn-cert: DFN-CERT-2019-0977
dfn-cert: DFN-CERT-2019-0974
dfn-cert: DFN-CERT-2019-0971
dfn-cert: DFN-CERT-2019-0969
dfn-cert: DFN-CERT-2019-0950
dfn-cert: DFN-CERT-2018-2399
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4507449)

Summary
This host is missing a critical security update according to Microsoft KB4507449

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24499
File checked:      C:\Windows\system32\Ntdll.dll
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code on a victim system, obtain information to further compromise the user's system and gain elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist as,
- Remote Desktop Services improperly handles clipboard redirection.
- Scripting Engine improperly handles objects in memory in Microsoft browsers.
- Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF), allow signing of SAML tokens with arbitrary symmetric keys.
- Windows GDI component improperly handles objects in memory.
- An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting.
- Kernel Information Disclosure Vulnerability (SWAPGS Attack).
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Microsoft Windows Multiple Vulnerabilities (KB4507449)
OID:1.3.6.1.4.1.25623.1.0.815403
Version used: 2022-08-09T10:11:17Z

References

```
cve: CVE-2019-0683
cve: CVE-2019-0887
cve: CVE-2019-1001
cve: CVE-2019-1004
cve: CVE-2019-1006
cve: CVE-2019-1056
cve: CVE-2019-1059
cve: CVE-2019-1063
cve: CVE-2019-1071
cve: CVE-2019-1073
cve: CVE-2019-1082
cve: CVE-2019-1085
cve: CVE-2019-1088
cve: CVE-2019-1089
cve: CVE-2019-1093
cve: CVE-2019-1094
cve: CVE-2019-1095
cve: CVE-2019-1096
cve: CVE-2019-1097
cve: CVE-2019-1098
cve: CVE-2019-1099
cve: CVE-2019-1100
cve: CVE-2019-1101
cve: CVE-2019-1102
cve: CVE-2019-1104
cve: CVE-2019-1108
cve: CVE-2019-1116
cve: CVE-2019-1125
cve: CVE-2019-1132
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4507449
cert-bund: CB-K19/0692
cert-bund: CB-K19/0595
cert-bund: CB-K19/0593
cert-bund: CB-K19/0591
cert-bund: CB-K19/0586
cert-bund: CB-K19/0212
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2445
dfn-cert: DFN-CERT-2019-2247
dfn-cert: DFN-CERT-2019-2127
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-2096
dfn-cert: DFN-CERT-2019-2007
dfn-cert: DFN-CERT-2019-1987
dfn-cert: DFN-CERT-2019-1985
dfn-cert: DFN-CERT-2019-1907
dfn-cert: DFN-CERT-2019-1855
dfn-cert: DFN-CERT-2019-1843
dfn-cert: DFN-CERT-2019-1823
dfn-cert: DFN-CERT-2019-1808
dfn-cert: DFN-CERT-2019-1734
dfn-cert: DFN-CERT-2019-1725
dfn-cert: DFN-CERT-2019-1705
dfn-cert: DFN-CERT-2019-1702
dfn-cert: DFN-CERT-2019-1701
dfn-cert: DFN-CERT-2019-1699
dfn-cert: DFN-CERT-2019-1698
dfn-cert: DFN-CERT-2019-1697
dfn-cert: DFN-CERT-2019-1696
dfn-cert: DFN-CERT-2019-1689
dfn-cert: DFN-CERT-2019-1671
dfn-cert: DFN-CERT-2019-1664
dfn-cert: DFN-CERT-2019-1641
dfn-cert: DFN-CERT-2019-1613
dfn-cert: DFN-CERT-2019-1612
dfn-cert: DFN-CERT-2019-1609
dfn-cert: DFN-CERT-2019-1396
dfn-cert: DFN-CERT-2019-1392
dfn-cert: DFN-CERT-2019-1391
dfn-cert: DFN-CERT-2019-1387
dfn-cert: DFN-CERT-2019-1384
dfn-cert: DFN-CERT-2019-1383
dfn-cert: DFN-CERT-2019-0506
dfn-cert: DFN-CERT-2018-2399
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4503292)

Summary
This host is missing a critical security update according to Microsoft KB4503292

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24475
File checked:      C:\Windows\system32\Ntdll.dll
File version:      6.1.7601.17514
```

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow an attacker to execute arbitrary code, elevate privileges by escaping a sandbox, gain access to sensitive information, run processes and delete files and folders in an elevated context.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- Windows Event Viewer (eventvwr.msc) improperly parses XML input containing a reference to an external entity.
- Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system.
- Microsoft Speech API (SAPI) improperly handles text-to-speech (TTS) input.
- Windows GDI component improperly discloses the contents of its memory.
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4503292)`
OID:1.3.6.1.4.1.25623.1.0.815208
Version used: `2023-10-27T16:11:32Z`

References
```
cve: CVE-2017-8533
cve: CVE-2019-0713
cve: CVE-2019-0722
cve: CVE-2019-0888
cve: CVE-2019-0904
cve: CVE-2019-0905
cve: CVE-2019-0906
cve: CVE-2019-0907
cve: CVE-2019-0908
cve: CVE-2019-0909
cve: CVE-2019-0920
cve: CVE-2019-0941
cve: CVE-2019-0943
cve: CVE-2019-0948
cve: CVE-2019-0960
cve: CVE-2019-0968
cve: CVE-2019-0972
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2019-0973
cve: CVE-2019-0974
cve: CVE-2019-0977
cve: CVE-2019-0984
cve: CVE-2019-0985
cve: CVE-2019-0986
cve: CVE-2019-0988
cve: CVE-2019-1005
cve: CVE-2019-1009
cve: CVE-2019-1010
cve: CVE-2019-1011
cve: CVE-2019-1012
cve: CVE-2019-1013
cve: CVE-2019-1014
cve: CVE-2019-1015
cve: CVE-2019-1016
cve: CVE-2019-1017
cve: CVE-2019-1019
cve: CVE-2019-1025
cve: CVE-2019-1028
cve: CVE-2019-1038
cve: CVE-2019-1039
cve: CVE-2019-1040
cve: CVE-2019-1043
cve: CVE-2019-1045
cve: CVE-2019-1046
cve: CVE-2019-1047
cve: CVE-2019-1048
cve: CVE-2019-1049
cve: CVE-2019-1053
cve: CVE-2019-1055
cve: CVE-2019-1080
cve: CVE-2019-1081
url: https://support.microsoft.com/en-us/help/4503292/
cert-bund: CB-K19/0500
cert-bund: CB-K19/0499
cert-bund: CB-K19/0497
cert-bund: CB-K17/0993
cert-bund: CB-K17/0992
dfn-cert: DFN-CERT-2019-1188
dfn-cert: DFN-CERT-2019-1186
dfn-cert: DFN-CERT-2019-1178
dfn-cert: DFN-CERT-2017-1023
dfn-cert: DFN-CERT-2017-1022
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4493472)

Summary
This host is missing a critical security update according to Microsoft KB4493472

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24408
File checked:      C:\Windows\system32\Ntdll.dll
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code on a victim system, obtain information to further compromise the user's system, gain elevated privileges, bypass security features and cause denial of service.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist in,
- The IOleCvt interface improperly renders ASP webpage content.
- Windows Jet Database Engine improperly handles objects in memory.
- Windows GDI component improperly discloses the contents of its memory.
- The win32k component improperly provides kernel information.
- Speculative execution side-channel vulnerabilities.
- Error in Various Windows components.
Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4493472)`
OID:1.3.6.1.4.1.25623.1.0.815033
Version used: `2023-10-27T16:11:32Z`

References
```
cve: CVE-2017-5753
cve: CVE-2017-5715
cve: CVE-2017-5754
cve: CVE-2019-0671
cve: CVE-2019-0673
cve: CVE-2019-0674
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2019-0730
cve: CVE-2019-0731
cve: CVE-2019-0732
cve: CVE-2019-0735
cve: CVE-2019-0752
cve: CVE-2019-0753
cve: CVE-2019-0764
cve: CVE-2019-0791
cve: CVE-2019-0792
cve: CVE-2019-0793
cve: CVE-2019-0794
cve: CVE-2019-0795
cve: CVE-2019-0796
cve: CVE-2019-0802
cve: CVE-2019-0803
cve: CVE-2019-0805
cve: CVE-2019-0835
cve: CVE-2019-0836
cve: CVE-2019-0838
cve: CVE-2019-0839
cve: CVE-2019-0842
cve: CVE-2019-0844
cve: CVE-2019-0845
cve: CVE-2019-0846
cve: CVE-2019-0847
cve: CVE-2019-0848
cve: CVE-2019-0849
cve: CVE-2019-0851
cve: CVE-2019-0853
cve: CVE-2019-0856
cve: CVE-2019-0859
cve: CVE-2019-0862
cve: CVE-2019-0877
cve: CVE-2019-0879
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4493472
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-0103
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K20/0324
cert-bund: CB-K19/0774
cert-bund: CB-K19/0298
cert-bund: CB-K19/0297
cert-bund: CB-K19/0296
cert-bund: CB-K19/0137
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/1140
cert-bund: CB-K18/0898
cert-bund: CB-K18/0654
cert-bund: CB-K18/0651
cert-bund: CB-K18/0635
cert-bund: CB-K18/0601
cert-bund: CB-K18/0557
cert-bund: CB-K18/0551
cert-bund: CB-K18/0518
cert-bund: CB-K18/0472
cert-bund: CB-K18/0463
cert-bund: CB-K18/0398
cert-bund: CB-K18/0381
cert-bund: CB-K18/0370
cert-bund: CB-K18/0367
cert-bund: CB-K18/0356
cert-bund: CB-K18/0348
cert-bund: CB-K18/0347
cert-bund: CB-K18/0346
cert-bund: CB-K18/0338
cert-bund: CB-K18/0283
cert-bund: CB-K18/0257
cert-bund: CB-K18/0250
cert-bund: CB-K18/0244
cert-bund: CB-K18/0207
cert-bund: CB-K18/0184
cert-bund: CB-K18/0177
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0148
cert-bund: CB-K18/0129
cert-bund: CB-K18/0099
cert-bund: CB-K18/0094
cert-bund: CB-K18/0054
cert-bund: CB-K18/0051
cert-bund: CB-K18/0049
cert-bund: CB-K18/0046
cert-bund: CB-K18/0040
cert-bund: CB-K18/0039
cert-bund: CB-K18/0023
cert-bund: CB-K18/0022
cert-bund: CB-K18/0021
cert-bund: CB-K18/0020
cert-bund: CB-K18/0017
cert-bund: CB-K18/0016
cert-bund: CB-K18/0010
cert-bund: CB-K18/0009
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/2117
cert-bund: CB-K17/2113
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1377
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-0879
dfn-cert: DFN-CERT-2023-0877
dfn-cert: DFN-CERT-2023-0876
dfn-cert: DFN-CERT-2023-0848
dfn-cert: DFN-CERT-2023-0795
dfn-cert: DFN-CERT-2023-0794
dfn-cert: DFN-CERT-2023-0793
dfn-cert: DFN-CERT-2023-0507
dfn-cert: DFN-CERT-2022-0531
dfn-cert: DFN-CERT-2020-1783
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-1987
dfn-cert: DFN-CERT-2019-1985
dfn-cert: DFN-CERT-2019-1837
dfn-cert: DFN-CERT-2019-1415
dfn-cert: DFN-CERT-2019-1235
dfn-cert: DFN-CERT-2019-1150
dfn-cert: DFN-CERT-2019-0725
dfn-cert: DFN-CERT-2019-0724
dfn-cert: DFN-CERT-2019-0720
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0613
dfn-cert: DFN-CERT-2019-0310
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2465
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1819
dfn-cert: DFN-CERT-2018-1794
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1726
dfn-cert: DFN-CERT-2018-1550
dfn-cert: DFN-CERT-2018-1504
dfn-cert: DFN-CERT-2018-1500
dfn-cert: DFN-CERT-2018-1494
dfn-cert: DFN-CERT-2018-1493
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1386
dfn-cert: DFN-CERT-2018-1385
dfn-cert: DFN-CERT-2018-1364
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1108
dfn-cert: DFN-CERT-2018-1032
dfn-cert: DFN-CERT-2018-1008
dfn-cert: DFN-CERT-2018-0991
dfn-cert: DFN-CERT-2018-0988
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0878
dfn-cert: DFN-CERT-2018-0857
dfn-cert: DFN-CERT-2018-0821
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0815
dfn-cert: DFN-CERT-2018-0808
dfn-cert: DFN-CERT-2018-0799
dfn-cert: DFN-CERT-2018-0796
dfn-cert: DFN-CERT-2018-0794
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0728
dfn-cert: DFN-CERT-2018-0682
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0625
dfn-cert: DFN-CERT-2018-0605
dfn-cert: DFN-CERT-2018-0598
dfn-cert: DFN-CERT-2018-0552
dfn-cert: DFN-CERT-2018-0510
dfn-cert: DFN-CERT-2018-0499
dfn-cert: DFN-CERT-2018-0427
dfn-cert: DFN-CERT-2018-0410
dfn-cert: DFN-CERT-2018-0397
dfn-cert: DFN-CERT-2018-0394
dfn-cert: DFN-CERT-2018-0382
dfn-cert: DFN-CERT-2018-0377
dfn-cert: DFN-CERT-2018-0375
dfn-cert: DFN-CERT-2018-0372
dfn-cert: DFN-CERT-2018-0367
dfn-cert: DFN-CERT-2018-0310
dfn-cert: DFN-CERT-2018-0276
dfn-cert: DFN-CERT-2018-0267
dfn-cert: DFN-CERT-2018-0262
dfn-cert: DFN-CERT-2018-0224
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0194
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0167
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0163
dfn-cert: DFN-CERT-2018-0137
dfn-cert: DFN-CERT-2018-0104
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2018-0066
dfn-cert: DFN-CERT-2018-0058
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0053
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0044
dfn-cert: DFN-CERT-2018-0031
dfn-cert: DFN-CERT-2018-0030
dfn-cert: DFN-CERT-2018-0029
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2018-0024
dfn-cert: DFN-CERT-2018-0022
dfn-cert: DFN-CERT-2018-0020
dfn-cert: DFN-CERT-2018-0019
dfn-cert: DFN-CERT-2017-2211
dfn-cert: DFN-CERT-2017-2210
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4489878)

Summary
This host is missing a critical security update according to Microsoft KB4489878

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24387
File checked:       C:\Windows\system32\Ntdll.dll
File version:       6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code on a victim system, obtain information to further compromise the user's system, gain elevated privileges, bypass security features and cause denial of service.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist in,
- Event Viewer from showing Network Interface Cards events and
- Various Windows components.

Please see the references for more information about the vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4489878)`
OID:1.3.6.1.4.1.25623.1.0.814936
Version used: `2023-10-27T16:11:32Z`

References

```
cve: CVE-2019-0601
cve: CVE-2019-0603
cve: CVE-2019-0609
cve: CVE-2019-0614
cve: CVE-2019-0617
cve: CVE-2019-0665
cve: CVE-2019-0666
cve: CVE-2019-0667
cve: CVE-2019-0680
cve: CVE-2019-0683
cve: CVE-2019-0690
cve: CVE-2019-0702
cve: CVE-2019-0703
cve: CVE-2019-0704
cve: CVE-2019-0746
cve: CVE-2019-0754
cve: CVE-2019-0755
cve: CVE-2019-0756
cve: CVE-2019-0759
cve: CVE-2019-0761
cve: CVE-2019-0762
cve: CVE-2019-0763
cve: CVE-2019-0765
cve: CVE-2019-0767
cve: CVE-2019-0772
cve: CVE-2019-0774
cve: CVE-2019-0775
cve: CVE-2019-0780
cve: CVE-2019-0782
cve: CVE-2019-0783
cve: CVE-2019-0784
cve: CVE-2019-0808
cve: CVE-2019-0821
cisa: Known Exploited Vulnerability (KEV) catalog
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4489878
url: http://www.securityfocus.com/bid/107285
cert-bund: CB-K19/0218
cert-bund: CB-K19/0217
cert-bund: CB-K19/0216
cert-bund: CB-K19/0212
cert-bund: CB-K19/0131
dfn-cert: DFN-CERT-2019-0521
dfn-cert: DFN-CERT-2019-0515
dfn-cert: DFN-CERT-2019-0507
dfn-cert: DFN-CERT-2019-0506
dfn-cert: DFN-CERT-2019-0311
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4462923)

Summary
This host is missing a critical security update according to Microsoft KB4462923

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24260
File checked:      C:\Windows\system32\Gdi32.dll
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to run arbitrary code, bypass security restrictions, gain the same user rights as the current user, obtain information to further compromise the user's system, improperly discloses file information and escalate privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- Windows Win32k component fails to properly handle objects in memory.
- Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system.
- Microsoft XML Core Services MSXML parser improperly processes user input.
- Internet Explorer improperly accesses objects in memory.

. . . continues on next page . . .

... continued from previous page ...

- Filter Manager improperly handles objects in memory.
- Windows TCP/IP stack improperly handles fragmented IP packets.
- Windows Media Player improperly discloses file information.
- Windows Graphics Device Interface (GDI) improperly handles objects in memory.
- DirectX Graphics Kernel (DXGKRNL) driver improperly handles objects in memory.
- Windows kernel improperly handles objects in memory.
- Windows Theme API does not properly decompress files.
- NTFS improperly checks access.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4462923)`
OID:1.3.6.1.4.1.25623.1.0.814084
Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-8320
cve: CVE-2018-8330
cve: CVE-2018-8333
cve: CVE-2018-8411
cve: CVE-2018-8413
cve: CVE-2018-8423
cve: CVE-2018-8432
cve: CVE-2018-8453
cve: CVE-2018-8460
cve: CVE-2018-8472
cve: CVE-2018-8481
cve: CVE-2018-8482
cve: CVE-2018-8486
cve: CVE-2018-8489
cve: CVE-2018-8491
cve: CVE-2018-8494
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4462923
cert-bund: CB-K18/0992
dfn-cert: DFN-CERT-2018-2059
dfn-cert: DFN-CERT-2018-2058
dfn-cert: DFN-CERT-2018-2055
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4457144)

Summary

This host is missing a critical security update according to Microsoft KB4457144.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable range:  Less than 11.0.9600.19130
File checked:      C:\Windows\system32\Urlmon.dll
File version:      8.0.7601.17514
```

Impact

Successful exploitation will allow an attacker to crash the affected system, execute arbitrary code on the host operating system, disclose contents of System memory and also read privileged data across trust boundaries.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit/x64-based Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- Denial of service vulnerability (named 'FragmentSmack').
- Hyper-V on a host server fails to properly validate guest operating system user input.
- Windows bowser.sys kernel-mode driver fails to properly handle objects in memory.
- Browser scripting engine improperly handle object types.
- Windows font library improperly handles specially crafted embedded fonts.
- Windows kernel improperly handles objects in memory.
- Microsoft JET Database Engine improperly handles objects in memory.
- Windows Kernel API improperly handles registry objects in memory.
- Windows kernel fails to properly initialize a memory address.
- MSXML parser improperly processes user input.
- Windows GDI component improperly handles objects in memory.
- Windows GDI component improperly discloses the contents of its memory.
- Windows Graphics component improperly handles objects in memory.
- Windows improperly handles calls to Advanced Local Procedure Call (ALPC).
- Internet Explorer improperly accesses objects in memory.
- Scripting engine improperly handles objects in memory.
- Windows improperly parses files.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4457144)`

OID:1.3.6.1.4.1.25623.1.0.814015

Version used: `2023-07-20T05:05:17Z`

References

`cve: CVE-2018-5391`

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2018-8271
cve: CVE-2018-8315
cve: CVE-2018-8332
cve: CVE-2018-8336
cve: CVE-2018-8392
cve: CVE-2018-8393
cve: CVE-2018-8410
cve: CVE-2018-8419
cve: CVE-2018-8420
cve: CVE-2018-8422
cve: CVE-2018-8424
cve: CVE-2018-8433
cve: CVE-2018-8434
cve: CVE-2018-8440
cve: CVE-2018-8442
cve: CVE-2018-8443
cve: CVE-2018-8446
cve: CVE-2018-8447
cve: CVE-2018-8452
cve: CVE-2018-8457
cve: CVE-2018-8468
cve: CVE-2018-8470
cve: CVE-2018-8475
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4457144
cert-bund: WID-SEC-2023-0508
cert-bund: CB-K18/0913
cert-bund: CB-K18/0854
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-0562
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0453
dfn-cert: DFN-CERT-2019-0442
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2018-2398
dfn-cert: DFN-CERT-2018-2366
dfn-cert: DFN-CERT-2018-2335
dfn-cert: DFN-CERT-2018-2260
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-2118
dfn-cert: DFN-CERT-2018-2117
dfn-cert: DFN-CERT-2018-2063
dfn-cert: DFN-CERT-2018-1943
dfn-cert: DFN-CERT-2018-1857
dfn-cert: DFN-CERT-2018-1850
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1847
dfn-cert: DFN-CERT-2018-1846
dfn-cert: DFN-CERT-2018-1845
dfn-cert: DFN-CERT-2018-1782
dfn-cert: DFN-CERT-2018-1730
dfn-cert: DFN-CERT-2018-1670
dfn-cert: DFN-CERT-2018-1661
dfn-cert: DFN-CERT-2018-1657
dfn-cert: DFN-CERT-2018-1635
dfn-cert: DFN-CERT-2018-1634
dfn-cert: DFN-CERT-2018-1632
dfn-cert: DFN-CERT-2018-1626
dfn-cert: DFN-CERT-2018-1617
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4343900)

Summary
This host is missing a critical security update according to Microsoft KB4343900

Vulnerability Detection Result

```
Vulnerable range:   Less than 11.0.9600.19101
File checked:       C:\Windows\system32\Mshtml.dll
File version:       8.0.7601.17514
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code, run processes in an elevated context, obtain information to further compromise the user's system, trick a user into believing that the user was on a legitimate website, read privileged data across trust boundaries and also bypass certain security restrictions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- A new speculative execution side channel vulnerability known as L1 Terminal Fault.
- Internet Explorer improperly validates hyperlinks before loading executable libraries.
- Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.
- NDIS fails to check the length of a buffer prior to copying memory to it.

. . . continues on next page . . .

. . . continued from previous page . . .

- Windows font library improperly handles specially crafted embedded fonts.
- An improper processing for a .LNK file.
- 'Microsoft COM for Windows' fails to properly handle serialized objects.
- Microsoft browsers improperly allow cross-frame interaction.
- Microsoft browsers allowing sandbox escape.
- Microsoft Edge improperly handles redirect requests and specific HTML content.
- Microsoft .NET Framework improperly access information in multi-tenant environments.
- WebAudio Library improperly handles audio requests.
- Windows GDI component improperly discloses the contents of its memory.
- Windows PDF Library improperly handles objects in memory.
- Windows Shell does not properly validate file paths.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4343900)`
OID:1.3.6.1.4.1.25623.1.0.813845
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2018-3615
cve: CVE-2018-3620
cve: CVE-2018-3646
cve: CVE-2018-8316
cve: CVE-2018-8339
cve: CVE-2018-8341
cve: CVE-2018-8342
cve: CVE-2018-8343
cve: CVE-2018-8345
cve: CVE-2018-8348
cve: CVE-2018-8349
cve: CVE-2018-8344
cve: CVE-2018-8351
cve: CVE-2018-8353
cve: CVE-2018-8355
cve: CVE-2018-8346
cve: CVE-2018-8371
cve: CVE-2018-8372
cve: CVE-2018-8373
cve: CVE-2018-8385
cve: CVE-2018-8389
cve: CVE-2018-8394
cve: CVE-2018-8396
cve: CVE-2018-8397
cve: CVE-2018-8398
cve: CVE-2018-8403
cve: CVE-2018-8404
cisa: Known Exploited Vulnerability (KEV) catalog
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4343900
cert-bund: CB-K19/0047
cert-bund: CB-K18/1050
cert-bund: CB-K18/0867
cert-bund: CB-K18/0863
cert-bund: CB-K18/0862
cert-bund: CB-K18/0861
cert-bund: CB-K18/0858
dfn-cert: DFN-CERT-2019-0740
dfn-cert: DFN-CERT-2019-0108
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0004
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2217
dfn-cert: DFN-CERT-2018-2182
dfn-cert: DFN-CERT-2018-2072
dfn-cert: DFN-CERT-2018-2066
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1863
dfn-cert: DFN-CERT-2018-1822
dfn-cert: DFN-CERT-2018-1806
dfn-cert: DFN-CERT-2018-1782
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1722
dfn-cert: DFN-CERT-2018-1699
dfn-cert: DFN-CERT-2018-1677
dfn-cert: DFN-CERT-2018-1670
dfn-cert: DFN-CERT-2018-1666
dfn-cert: DFN-CERT-2018-1665
dfn-cert: DFN-CERT-2018-1661
dfn-cert: DFN-CERT-2018-1657
dfn-cert: DFN-CERT-2018-1656
dfn-cert: DFN-CERT-2018-1654
dfn-cert: DFN-CERT-2018-1653
dfn-cert: DFN-CERT-2018-1652
dfn-cert: DFN-CERT-2018-1651
dfn-cert: DFN-CERT-2018-1650
dfn-cert: DFN-CERT-2018-1637
dfn-cert: DFN-CERT-2018-1634
dfn-cert: DFN-CERT-2018-1632
dfn-cert: DFN-CERT-2018-1631
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-1629
dfn-cert: DFN-CERT-2018-1627
dfn-cert: DFN-CERT-2018-1625
dfn-cert: DFN-CERT-2018-1624
dfn-cert: DFN-CERT-2018-1623
dfn-cert: DFN-CERT-2018-1622
dfn-cert: DFN-CERT-2018-1621
dfn-cert: DFN-CERT-2018-1619
dfn-cert: DFN-CERT-2018-1617
dfn-cert: DFN-CERT-2018-1615
dfn-cert: DFN-CERT-2018-1614
dfn-cert: DFN-CERT-2018-1612
dfn-cert: DFN-CERT-2018-1606
dfn-cert: DFN-CERT-2018-1605
dfn-cert: DFN-CERT-2018-1601
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4093118)

Summary
This host is missing a critical security update according to Microsoft KB4093118

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\mshtml.dll
File version:     8.0.7601.17514
Vulnerable range:  Less than 11.0.9600.18978
```

Impact
Successful exploitation will allow an attacker to take control of the affected system, obtain information to further compromise the user's system, execute arbitrary code, retrieve the memory address of a kernel object, cause a target system to stop responding.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- When the Windows font library improperly handles specially crafted embedded fonts.
- When Internet Explorer improperly accesses objects in memory.
- When the Windows kernel fails to properly initialize a memory address.

... continues on next page ...

. . . continued from previous page . . .

- When the scripting engine does not properly handle objects in memory in Internet Explorer.
- In Windows Adobe Type Manager Font Driver (ATMFD.
- In the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass.
- In the way that Windows SNMP Service handles malformed SNMP traps.
- When the Windows kernel improperly handles objects in memory.
- In the way that the VBScript engine handles objects in memory.
- In the way that Windows handles objects in memory.
- In Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests.
- In the Microsoft JET Database Engine that could allow remote code execution on an affected system.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4093118)`
OID:1.3.6.1.4.1.25623.1.0.812863
Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-0870
cve: CVE-2018-0887
cve: CVE-2018-8116
cve: CVE-2018-0960
cve: CVE-2018-0967
cve: CVE-2018-0969
cve: CVE-2018-0970
cve: CVE-2018-0971
cve: CVE-2018-0972
cve: CVE-2018-0973
cve: CVE-2018-0974
cve: CVE-2018-0975
cve: CVE-2018-0976
cve: CVE-2018-0981
cve: CVE-2018-0987
cve: CVE-2018-0988
cve: CVE-2018-0989
cve: CVE-2018-0991
cve: CVE-2018-1003
cve: CVE-2018-1004
cve: CVE-2018-1008
cve: CVE-2018-1010
cve: CVE-2018-1012
cve: CVE-2018-1013
cve: CVE-2018-1015
cve: CVE-2018-1016
cve: CVE-2018-1018
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-1020
cve: CVE-2018-0996
cve: CVE-2018-0997
cve: CVE-2018-1000
cve: CVE-2018-1001
url: https://support.microsoft.com/en-us/help/4093118
cert-bund: CB-K18/0586
cert-bund: CB-K18/0585
dfn-cert: DFN-CERT-2018-0680
dfn-cert: DFN-CERT-2018-0678
```

High (CVSS: 8.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4038777)

Summary
This host is missing a critical security update according to Microsoft KB4038777

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\win32spl.dll
File version:     6.1.7601.17514
Vulnerable range:  Less than 6.1.7601.23889
```

Impact
Successful exploitation will allow an attacker to gain access to potentially sensitive information, perform a man-in-the-middle attack and force a user's computer to unknowingly route traffic through the attacker's computer, execute arbitrary code on the target, embed an ActiveX control marked safe for initialization, take complete control of the affected system and read arbitrary files on the affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An error when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system.
- An issue when the Windows kernel fails to properly initialize a memory address.
- An error when the Windows kernel improperly handles objects in memory.
- An error in Microsoft's implementation of the Bluetooth stack.

. . . continues on next page . . .

. . . continued from previous page . . .

- An error in the way that Microsoft browser JavaScript engines render content when handling objects in memory.
- An error when Windows Uniscribe improperly discloses the contents of its memory.
- An error due to the way Windows Uniscribe handles objects in memory.
- An error when Microsoft browsers improperly access objects in memory.
- An error when Internet Explorer improperly handles specific HTML content.
- An error in Microsoft browsers due to improper parent domain verification in certain functionality.
- An error in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system.
- An error when the Windows GDI+ component improperly discloses kernel memory addresses.
- An error in Windows when the Windows kernel-mode driver fails to properly handle objects in memory.
- An error when Windows Shell does not properly validate file copy destinations.
- An error in Windows kernel.
- An error when the Windows font library improperly handles specially crafted embedded fonts.
- An error in the Microsoft Common Console Document.
- An error in Windows when the Win32k component fails to properly handle objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4038777)`
OID:1.3.6.1.4.1.25623.1.0.811746
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2017-0161
cve: CVE-2017-8719
cve: CVE-2017-8720
cve: CVE-2017-8628
cve: CVE-2017-8733
cve: CVE-2017-8736
cve: CVE-2017-8675
cve: CVE-2017-8676
cve: CVE-2017-8741
cve: CVE-2017-8677
cve: CVE-2017-8678
cve: CVE-2017-8747
cve: CVE-2017-8748
cve: CVE-2017-8679
cve: CVE-2017-8680
cve: CVE-2017-8681
cve: CVE-2017-8749
cve: CVE-2017-8750
cve: CVE-2017-8682
cve: CVE-2017-8683
cve: CVE-2017-8684
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-8685
cve: CVE-2017-8687
cve: CVE-2017-8688
cve: CVE-2017-8696
cve: CVE-2017-8699
cve: CVE-2017-8707
cve: CVE-2017-8708
cve: CVE-2017-8709
cve: CVE-2017-8710
cve: CVE-2017-8695
url: https://support.microsoft.com/en-us/help/4038777
url: http://www.securityfocus.com/bid/100728
url: http://www.securityfocus.com/bid/100744
url: http://www.securityfocus.com/bid/100737
url: http://www.securityfocus.com/bid/100743
url: http://www.securityfocus.com/bid/100752
url: http://www.securityfocus.com/bid/100755
url: http://www.securityfocus.com/bid/100764
url: http://www.securityfocus.com/bid/100767
url: http://www.securityfocus.com/bid/100769
url: http://www.securityfocus.com/bid/100765
url: http://www.securityfocus.com/bid/100766
url: http://www.securityfocus.com/bid/100720
url: http://www.securityfocus.com/bid/100722
url: http://www.securityfocus.com/bid/100727
url: http://www.securityfocus.com/bid/100770
url: http://www.securityfocus.com/bid/100771
url: http://www.securityfocus.com/bid/100772
url: http://www.securityfocus.com/bid/100781
url: http://www.securityfocus.com/bid/100782
url: http://www.securityfocus.com/bid/100724
url: http://www.securityfocus.com/bid/100736
url: http://www.securityfocus.com/bid/100756
url: http://www.securityfocus.com/bid/100780
url: http://www.securityfocus.com/bid/100783
url: http://www.securityfocus.com/bid/100790
url: http://www.securityfocus.com/bid/100791
url: http://www.securityfocus.com/bid/100792
url: http://www.securityfocus.com/bid/100793
url: http://www.securityfocus.com/bid/100773
cert-bund: CB-K17/1570
cert-bund: CB-K17/1553
cert-bund: CB-K17/1550
cert-bund: CB-K17/1548
cert-bund: CB-K17/1547
dfn-cert: DFN-CERT-2017-1634
dfn-cert: DFN-CERT-2017-1614
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1613
dfn-cert: DFN-CERT-2017-1612
dfn-cert: DFN-CERT-2017-1611
```

High (CVSS: 8.8)
NVT: Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (3124584)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-005.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Gdi32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19091
```

Impact
Successful exploitation will allow an attacker to bypass Address Space Layout Randomization (ASLR) protection mechanisms and gain access to sensitive informationand to execute arbitrary code in the context of the currently logged-in user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
Multiple flaws are due to:
- A security feature bypass vulnerability exists in the way Windows graphics device interface handles objects in memory.
- An error in the way Windows handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel-Mode Drivers Remote Code Execution Vulnerabilities (31.`

. . . continues on next page . . .

. . . continued from previous page . . .

↪..
OID:1.3.6.1.4.1.25623.1.0.807028
Version used: 2023-07-20T05:05:17Z

References

```
cve: CVE-2016-0009
cve: CVE-2016-0008
url: https://support.microsoft.com/en-us/kb/3124001
url: https://support.microsoft.com/en-us/kb/3124000
url: https://technet.microsoft.com/library/security/MS16-005
cert-bund: CB-K16/0057
```

High (CVSS: 8.8)
NVT: Microsoft Uniscribe Remote Code Execution Vulnerability (3204063)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS16-147.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Usp10.dll
File version:     1.626.7601.17514
Vulnerable range: Less than 1.626.7601.23585
```

Impact

Successful exploitation will allow an attacker to take control of the affected system. An attacker could then:
- install programs
- view, change, or delete data
- or create new accounts with full user rights.
Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Solution:

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2016

Vulnerability Insight

The flaw exists due to the way Windows Uniscribe handles objects in the memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Uniscribe Remote Code Execution Vulnerability (3204063)`

OID:1.3.6.1.4.1.25623.1.0.809832

Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-7274
url: https://support.microsoft.com/en-us/kb/3204063
url: https://technet.microsoft.com/library/security/MS16-147
cert-bund: CB-K16/1959
```

High (CVSS: 8.8)

NVT: Microsoft Uniscribe Multiple Vulnerabilities (4013076)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS17-011.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Usp10.dll
File version:     1.626.7601.17514
Vulnerable range: Less than 1.626.7601.23688
```

Impact

Successful exploitation will allow an attacker to take control of the affected system, also to obtain information to further compromise the user's system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

. . . continues on next page . . .

... continued from previous page ...

- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2016

Vulnerability Insight

Multiple flaws exist due to:

- The way Windows Uniscribe handles objects in memory.
- When Windows Uniscribe improperly discloses the contents of its memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Uniscribe Multiple Vulnerabilities (4013076)`

OID:1.3.6.1.4.1.25623.1.0.810812

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2017-0072
cve: CVE-2017-0083
cve: CVE-2017-0084
cve: CVE-2017-0085
cve: CVE-2017-0086
cve: CVE-2017-0087
cve: CVE-2017-0088
cve: CVE-2017-0089
cve: CVE-2017-0090
cve: CVE-2017-0091
cve: CVE-2017-0092
cve: CVE-2017-0111
cve: CVE-2017-0112
cve: CVE-2017-0113
cve: CVE-2017-0114
cve: CVE-2017-0115
cve: CVE-2017-0116
cve: CVE-2017-0117
cve: CVE-2017-0118
cve: CVE-2017-0119
cve: CVE-2017-0120
cve: CVE-2017-0121
cve: CVE-2017-0122
cve: CVE-2017-0123
cve: CVE-2017-0124
cve: CVE-2017-0125
cve: CVE-2017-0126
cve: CVE-2017-0127
cve: CVE-2017-0128
url: https://support.microsoft.com/en-us/kb/
url: http://www.securityfocus.com/bid/96599
```

... continues on next page ...

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/96608
url: http://www.securityfocus.com/bid/96610
url: http://www.securityfocus.com/bid/96652
url: http://www.securityfocus.com/bid/96603
url: http://www.securityfocus.com/bid/96604
url: http://www.securityfocus.com/bid/96605
url: http://www.securityfocus.com/bid/96606
url: http://www.securityfocus.com/bid/96607
url: http://www.securityfocus.com/bid/96657
url: http://www.securityfocus.com/bid/96676
url: http://www.securityfocus.com/bid/96658
url: http://www.securityfocus.com/bid/96659
url: http://www.securityfocus.com/bid/96660
url: http://www.securityfocus.com/bid/96661
url: http://www.securityfocus.com/bid/96663
url: http://www.securityfocus.com/bid/96665
url: http://www.securityfocus.com/bid/96679
url: http://www.securityfocus.com/bid/96680
url: http://www.securityfocus.com/bid/96666
url: http://www.securityfocus.com/bid/96667
url: http://www.securityfocus.com/bid/96678
url: http://www.securityfocus.com/bid/96668
url: http://www.securityfocus.com/bid/96669
url: http://www.securityfocus.com/bid/96670
url: http://www.securityfocus.com/bid/96672
url: http://www.securityfocus.com/bid/96673
url: http://www.securityfocus.com/bid/96674
url: http://www.securityfocus.com/bid/96675
url: https://technet.microsoft.com/library/security/MS17-011
cert-bund: CB-K17/0443
dfn-cert: DFN-CERT-2017-0451
```

High (CVSS: 8.8)
NVT: Microsoft .NET Framework Multiple Vulnerabilities (KB4483455)

Summary
This host is missing an important security update according to Microsoft KB4483455

Vulnerability Detection Result

```
Vulnerable range:  4.0.30319.30000 - 4.0.30319.36519
File checked:      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\system.dll
File version:      4.0.30319.34209
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow an attacker to bypass security logic intended to ensure that a user-provided URL belonged to a specific hostname or a subdomain of that hostname and run arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 4.5.2 on Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An error in .NET Framework when the software fails to check the source markup of a file.
- An error in certain .Net Framework API's in the way they parse URL's.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Multiple Vulnerabilities (KB4483455)`
OID:1.3.6.1.4.1.25623.1.0.814748
Version used: `2022-04-13T07:21:45Z`

References
```
cve: CVE-2019-0657
cve: CVE-2019-0613
url: https://support.microsoft.com/en-us/help/4483455
url: http://www.securityfocus.com/bid/106890
url: http://www.securityfocus.com/bid/106872
cert-bund: CB-K19/0136
cert-bund: CB-K19/0135
dfn-cert: DFN-CERT-2019-0363
dfn-cert: DFN-CERT-2019-0329
dfn-cert: DFN-CERT-2019-0318
```

High (CVSS: 8.8)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3204059)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-144.

Vulnerability Detection Result
```
File checked:     C:\Windows\system32\Mshtml.dll
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
File version:     8.0.7601.17514
Vulnerable range: Less than 11.0.9600.18538
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code in the context of the current user, also could gain the same user rights as the current user, and obtain information to further compromise the user's system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft Internet Explorer version 9.x/10.x/11.x.

Vulnerability Insight

Multiple flaws exist due to:
- The way that the affected components handle objects in memory.
- Microsoft browsers improperly accesses objects in memory.
- Microsoft browsers fail to correctly apply Same Origin Policy for scripts running inside Web Workers.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3204059)`
OID:1.3.6.1.4.1.25623.1.0.809833
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-7202
cve: CVE-2016-7278
cve: CVE-2016-7279
cve: CVE-2016-7281
cve: CVE-2016-7282
cve: CVE-2016-7283
cve: CVE-2016-7284
cve: CVE-2016-7287
url: https://support.microsoft.com/en-sg/kb/3204059
url: https://technet.microsoft.com/library/security/MS16-144
cert-bund: CB-K16/1949
cert-bund: CB-K16/1948
cert-bund: CB-K16/1744
```

High (CVSS: 8.8)
NVT: Microsoft Graphics Component Multiple Vulnerabilities (3204066)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-146.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Gdi32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23591
```

Impact
Successful exploitation will allow an attacker to take control of the affected system. An attacker could then:
- install programs
- view, change, or delete data
- or create new accounts with full user rights.

Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2016

Vulnerability Insight
Multiple flaws are due to:
- the windows GDI component improperly discloses the contents of its memory.
- the Windows Graphics component improperly handles objects in the memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Graphics Component Multiple Vulnerabilities (3204066)`
OID:1.3.6.1.4.1.25623.1.0.809831
Version used: `2023-07-20T05:05:17Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2016-7257
cve: CVE-2016-7272
cve: CVE-2016-7273
url: https://support.microsoft.com/en-us/kb/3204066
url: https://technet.microsoft.com/library/security/MS16-146
cert-bund: CB-K16/1959
cert-bund: CB-K16/1956
```

High (CVSS: 8.8)
NVT: Microsoft Graphics Component Multiple Vulnerabilities (3199120)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS16-132.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\fontsub.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23587
```

Impact

Successful exploitation will allow an attacker to install programs, view, change, or delete data, or create new accounts with full user rights, and to obtain information to further compromise the user's system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight

Multiple flaws are due to:

- the ATMFD component improperly discloses the contents of its memory.
- the Windows Animation Manager improperly handles objects in memory.
- the Windows font library improperly handles specially crafted embedded fonts.

. . . continues on next page . . .

... continued from previous page ...

- the Windows Media Foundation improperly handles objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Graphics Component Multiple Vulnerabilities (3199120)`
OID:1.3.6.1.4.1.25623.1.0.809466
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-7210
cve: CVE-2016-7205
cve: CVE-2016-7217
cve: CVE-2016-7256
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3199120
url: http://www.securityfocus.com/bid/94030
url: http://www.securityfocus.com/bid/94033
url: http://www.securityfocus.com/bid/94066
url: http://www.securityfocus.com/bid/94156
url: https://technet.microsoft.com/library/security/MS16-132
cert-bund: CB-K16/1747
```

High (CVSS: 8.8)
NVT: Microsoft Graphics Component Multiple Vulnerabilities (3156754)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS16-055.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Gdi32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23418
```

Impact

Successful exploitation will allow an attacker to obtain information to further compromise the user's system, and install programs view, change, or delete data, or create new accounts with full user rights.

Solution:

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64

... continues on next page ...

. . . continued from previous page . . .

- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight

Multiple flaws are due to:

- Windows GDI component improperly discloses the contents of its memory.
- Windows Imaging Component fails to properly handle objects in the memory.
- Windows GDI component fails to properly handle objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Graphics Component Multiple Vulnerabilities (3156754)`

OID:1.3.6.1.4.1.25623.1.0.807691

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0168
cve: CVE-2016-0169
cve: CVE-2016-0170
cve: CVE-2016-0184
cve: CVE-2016-0195
url: https://support.microsoft.com/en-us/kb/3156013
url: https://support.microsoft.com/en-us/kb/3156016
url: https://support.microsoft.com/en-us/kb/3156019
url: https://technet.microsoft.com/library/security/MS16-055
cert-bund: CB-K16/0701
```

High (CVSS: 8.8)

NVT: Microsoft Graphics Component Multiple Vulnerabilities (3148522)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS16-039.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23407
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attackers to execute arbitrary code and gain elevated privileges on the affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight
Multiple flaws exist due to:
- An error in kernel-mode driver which fails to properly handle objects in memory.
- An error in windows font library which improperly handles specially crafted embedded fonts.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Graphics Component Multiple Vulnerabilities (3148522)`
OID:1.3.6.1.4.1.25623.1.0.806699
Version used: `2023-07-20T05:05:17Z`

References
```
cve: CVE-2016-0143
cve: CVE-2016-0145
cve: CVE-2016-0165
cve: CVE-2016-0167
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3148522
url: https://technet.microsoft.com/library/security/MS16-039
url: https://technet.microsoft.com/en-us/library/security/MS16-039
cert-bund: CB-K16/0556
cert-bund: CB-K16/0546
cert-bund: CB-K16/0545
```

High (CVSS: 8.8)
NVT: Microsoft Graphic Fonts Multiple Vulnerabilities (3143148)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-026.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Atmfd.dll
File version:     5.1.2.230
Vulnerable range: Less than 5.1.2.247
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code. Failed exploit attempts will result in a denial-of-service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Graphic Fonts Multiple Vulnerabilities (3143148)`
OID:1.3.6.1.4.1.25623.1.0.807513
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0121
cve: CVE-2016-0120
url: https://support.microsoft.com/en-us/kb/3140735
url: https://technet.microsoft.com/library/security/MS16-026
cert-bund: CB-K16/0383
```

High (CVSS: 8.8)
NVT: Microsoft SMBv1 Server Authenticated Remote Code Execution Vulnerability (3185879)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-114.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\drivers\Srv.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23517
```

Impact
Successful exploitation will allow attacker to take complete control of an affected system. An attacker could then install, programs, view, change, or delete data or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight
An authenticated remote code execution vulnerability exists in Windows that is caused when Server Message Block (SMB) improperly handles certain logging activities, resulting in memory corruption.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft SMBv1 Server Authenticated Remote Code Execution Vulnerability (31858.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809225
Version used: `2024-06-21T05:05:42Z`

References

```
cve: CVE-2016-3345
url: https://support.microsoft.com/en-us/kb/3185879
url: http://www.securityfocus.com/bid/92859
url: https://technet.microsoft.com/library/security/MS16-114
cert-bund: CB-K16/1406
```

High (CVSS: 8.6)
NVT: Oracle Java SE Security Update (oct2021) 01 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability, integrity and confidentiality.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u301 (1.8.0.301) and earlier on Windows.

Vulnerability Insight
Multiple flaws are due to multiple errors in 'JavaFX' and 'Deployment' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Java SE Security Update (oct2021) 01 - Windows
OID:1.3.6.1.4.1.25623.1.0.818827
Version used: 2023-04-03T10:19:50Z

References

```
cve: CVE-2021-3517
cve: CVE-2021-35560
cve: CVE-2021-3522
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1152
cert-bund: WID-SEC-2023-0395
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-1113
cert-bund: WID-SEC-2022-0196
cert-bund: CB-K22/0239
cert-bund: CB-K22/0061
cert-bund: CB-K21/1082
cert-bund: CB-K21/0647
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K21/0450
dfn-cert: DFN-CERT-2023-2306
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0213
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0024
```

High (CVSS: 8.6)
NVT: Oracle Java SE Security Update (oct2021) 01 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability, integrity and confidentiality.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u301 (1.8.0.301) and earlier on Windows.

Vulnerability Insight
Multiple flaws are due to multiple errors in 'JavaFX' and 'Deployment' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Java SE Security Update (oct2021) 01 - Windows
OID:1.3.6.1.4.1.25623.1.0.818827
Version used: 2023-04-03T10:19:50Z

References

```
cve: CVE-2021-3517
cve: CVE-2021-35560
cve: CVE-2021-3522
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1152
cert-bund: WID-SEC-2023-0395
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-1113
cert-bund: WID-SEC-2022-0196
cert-bund: CB-K22/0239
cert-bund: CB-K22/0061
cert-bund: CB-K21/1082
cert-bund: CB-K21/0647
cert-bund: CB-K21/0450
dfn-cert: DFN-CERT-2023-2306
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0213
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0024
```

High (CVSS: 8.5)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5021291)

Summary
This host is missing an important security update according to Microsoft KB5021291

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.26262
File checked:       C:\Windows\system32\Ntoskrnl.exe
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to elevate privileges, disclose sensitive information, conduct remote code execution, bypass security restrictions, and conduct DoS attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An elevation of privilege vulnerability in Windows Fax Compose Form.

. . . continues on next page . . .

. . . continued from previous page . . .

- An elevation of privilege vulnerability in Windows Graphics Component.
- A Remote Code Execution vulnerability in Windows Contacts.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5021291)`

OID:1.3.6.1.4.1.25623.1.0.826811

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-41074
cve: CVE-2022-41077
cve: CVE-2022-41121
cve: CVE-2022-44666
cve: CVE-2022-44667
cve: CVE-2022-44668
cve: CVE-2022-44670
cve: CVE-2022-44673
cve: CVE-2022-44675
cve: CVE-2022-44676
cve: CVE-2022-44678
cve: CVE-2022-44681
cve: CVE-2022-44697
cve: CVE-2022-41076
cve: CVE-2022-41094
url: https://support.microsoft.com/en-us/help/5021291
cert-bund: WID-SEC-2022-2307
cert-bund: WID-SEC-2022-2303
dfn-cert: DFN-CERT-2022-2854
dfn-cert: DFN-CERT-2022-2847
```

High (CVSS: 8.3)

NVT: Oracle Java SE Security Updates - 01 - (cpujul2020) - Windows

Summary

Oracle Java SE is prone to a security vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u251 (1.8.0.251) and earlier.

Vulnerability Insight
The flaw exists due to an error in the 'JavaFX' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates - 01 - (cpujul2020) - Windows`
OID:1.3.6.1.4.1.25623.1.0.118162
Version used: `2024-02-26T14:36:40Z`

References
```
cve: CVE-2020-14664
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA
cert-bund: WID-SEC-2022-1522
cert-bund: CB-K20/0715
dfn-cert: DFN-CERT-2020-1531
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Update (cpuapr2020 - 01) - Linux

Summary
Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.8.0update_211
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jdk1.8.0_211
```

Impact
Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Oracle Java SE version 7u251 (1.7.0.251) and earlier, 8u241 (1.8.0.241) and earlier, 11.0.6 and earlier, 14.

Vulnerability Insight

Multiple flaws are due to errors in components Libraries, JSSE, Concurrency, Lightweight HTTP Server, Serialization and Security.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (cpuapr2020 - 01) - Linux`
OID:1.3.6.1.4.1.25623.1.0.816859
Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2020-2803
cve: CVE-2020-2805
cve: CVE-2020-2781
cve: CVE-2020-2830
cve: CVE-2020-2800
cve: CVE-2020-2773
cve: CVE-2020-2756
cve: CVE-2020-2757
url: https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1639
cert-bund: CB-K21/0279
cert-bund: CB-K20/0319
cert-bund: CB-K20/0312
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-1685
dfn-cert: DFN-CERT-2020-1425
dfn-cert: DFN-CERT-2020-0778
dfn-cert: DFN-CERT-2020-0771
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates - 01 - (cpujul2020) - Windows

Summary

Oracle Java SE is prone to a security vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:        C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u251 (1.8.0.251) and earlier.

Vulnerability Insight

The flaw exists due to an error in the 'JavaFX' component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Updates - 01 - (cpujul2020) - Windows`

OID:1.3.6.1.4.1.25623.1.0.118162

Version used: `2024-02-26T14:36:40Z`

References

```
cve: CVE-2020-14664
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA
cert-bund: WID-SEC-2022-1522
cert-bund: CB-K20/0715
dfn-cert: DFN-CERT-2020-1531
```

High (CVSS: 8.3)

NVT: Oracle Java SE Security Updates - 03 - (cpujul2020) - Windows

Summary

Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:      Apply the patch
Installation
path / port:        C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 7u261 (1.7.0.261) and earlier, 8u251 (1.8.0.251) and earlier, 11.0.7 and earlier, 14.0.1 and earlier on Windows.

Vulnerability Insight
Multiple flaws are due to errors in components Libraries, 2D, JAXP and JSSE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates - 03 - (cpujul2020) - Windows`
OID:1.3.6.1.4.1.25623.1.0.118166
Version used: `2024-02-26T14:36:40Z`

References
```
cve: CVE-2020-14583
cve: CVE-2020-14593
cve: CVE-2020-14621
cve: CVE-2020-14577
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1522
cert-bund: WID-SEC-2022-1285
cert-bund: CB-K20/1075
cert-bund: CB-K20/0715
cert-bund: CB-K20/0706
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-1762
dfn-cert: DFN-CERT-2020-1531
dfn-cert: DFN-CERT-2020-1529
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates - 03 - (cpujul2020) - Windows

Summary
Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 7u261 (1.7.0.261) and earlier, 8u251 (1.8.0.251) and earlier, 11.0.7 and earlier, 14.0.1 and earlier on Windows.

Vulnerability Insight

Multiple flaws are due to errors in components Libraries, 2D, JAXP and JSSE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Updates - 03 - (cpujul2020) - Windows`

OID:1.3.6.1.4.1.25623.1.0.118166

Version used: `2024-02-26T14:36:40Z`

References

```
cve: CVE-2020-14583
cve: CVE-2020-14593
cve: CVE-2020-14621
cve: CVE-2020-14577
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1522
cert-bund: WID-SEC-2022-1285
cert-bund: CB-K20/1075
cert-bund: CB-K20/0715
cert-bund: CB-K20/0706
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-1762
dfn-cert: DFN-CERT-2020-1531
dfn-cert: DFN-CERT-2020-1529
```

High (CVSS: 8.3)

NVT: Microsoft Group Policy Remote Code Execution Vulnerability (3000483)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-011.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow context-dependent to execute arbitrary code. Failed exploit attempts will result in a denial-of-service condition.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2

Vulnerability Insight

The flaw is due to remote code execution vulnerability in the way Group Policy receives and applies policy data if a domain-joined system is connected to a domain controller

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Group Policy Remote Code Execution Vulnerability (3000483)`

OID:1.3.6.1.4.1.25623.1.0.805448

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0008
url: https://support.microsoft.com/kb/3000483
url: http://www.securityfocus.com/bid/72477
url: https://technet.microsoft.com/library/security/ms15-011
cert-bund: CB-K15/0171
dfn-cert: DFN-CERT-2015-0175
```

High (CVSS: 8.1)

NVT: Microsoft Windows Print Spooler Components Multiple Vulnerabilities (3170005)

Summary

. . . continues on next page . . .

... continued from previous page ...

This host is missing a critical security update according to Microsoft Bulletin MS16-087

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Win32spl.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23488
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code and take control of an affected system, also allows local users to gain privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 for 32-bit/64-bit

Vulnerability Insight

Multiple flaws exist due to

- When the Windows Print Spooler service improperly allows arbitrary writing to the file system.
- An improper validation of print drivers while installing a printer from servers.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Print Spooler Components Multiple Vulnerabilities (3170005)`

OID:1.3.6.1.4.1.25623.1.0.808194

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3238
cve: CVE-2016-3239
url: https://support.microsoft.com/en-us/kb/3170005
url: http://www.securityfocus.com/bid/91609
url: http://www.securityfocus.com/bid/91612
url: https://technet.microsoft.com/library/security/MS16-087
cert-bund: CB-K16/1057
```

High (CVSS: 8.1)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010(WannaCrypt)

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23677
```

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows XP SP2 x64
- Microsoft Windows XP SP3 x86
- Microsoft Windows 8 x86/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests(WannaCrypt).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810810
Version used: `2023-07-14T16:09:27Z`

References
`cve: CVE-2017-0143`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-0144
cve: CVE-2017-0145
cve: CVE-2017-0146
cve: CVE-2017-0147
cve: CVE-2017-0148
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013078
url: http://www.securityfocus.com/bid/96703
url: http://www.securityfocus.com/bid/96704
url: http://www.securityfocus.com/bid/96705
url: http://www.securityfocus.com/bid/96707
url: http://www.securityfocus.com/bid/96709
url: http://www.securityfocus.com/bid/96706
url: https://technet.microsoft.com/library/security/MS17-010
url: http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
url: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-w
↪annacrypt-attacks
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448
```

High (CVSS: 8.1)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3096441)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-106.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: 8.0.7601.17000 - 8.0.7601.19002
```

Impact
Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws are due to:

. . . continues on next page . . .

. . . continued from previous page . . .

- Multiple improper handling memory objects,
- Improper permissions validation, allowing a script to be run with elevated privileges.
- An error in 'CAttrArray' object implementation.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3096441)`

OID:1.3.6.1.4.1.25623.1.0.805761

Version used: `2023-11-02T05:05:26Z`

References

```
cve: CVE-2015-2482
cve: CVE-2015-6042
cve: CVE-2015-6044
cve: CVE-2015-6046
cve: CVE-2015-6047
cve: CVE-2015-6048
cve: CVE-2015-6049
cve: CVE-2015-6050
cve: CVE-2015-6051
cve: CVE-2015-6052
cve: CVE-2015-6053
cve: CVE-2015-6055
cve: CVE-2015-6056
cve: CVE-2015-6059
cve: CVE-2015-6184
url: https://support.microsoft.com/en-us/kb/3096441
url: https://technet.microsoft.com/en-us/library/security/MS15-106
cert-bund: CB-K15/1507
cert-bund: CB-K15/1504
dfn-cert: DFN-CERT-2015-1586
dfn-cert: DFN-CERT-2015-1583
```

High (CVSS: 8.1)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (4013073)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS17-006.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: Less than 11.0.9600.18618
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attackers to gain elevated privileges, gain access to potentially sensitive information, execute arbitrary code in the context of the current user and conduct spoofing attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 9.x/10.x/11.x.

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors in the components handling objects in memory.
- Microsoft browsers improperly access objects in memory.
- An error in Microsoft browser which does not properly parse HTTP responses.
- Multiple errors in JScript and VBScript engines rendering when handling objects in memory.
- An error in Internet Explorer which does not properly enforce cross-domain policies.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (4013073)`
OID:1.3.6.1.4.1.25623.1.0.810625
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-0008
cve: CVE-2017-0009
cve: CVE-2017-0012
cve: CVE-2017-0018
cve: CVE-2017-0033
cve: CVE-2017-0037
cve: CVE-2017-0040
cve: CVE-2017-0049
cve: CVE-2017-0059
cve: CVE-2017-0130
cve: CVE-2017-0149
cve: CVE-2017-0154
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4013073
url: https://technet.microsoft.com/library/security/MS17-006
cert-bund: CB-K17/0439
cert-bund: CB-K17/0436
cert-bund: CB-K17/0338
dfn-cert: DFN-CERT-2017-0450
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0444
dfn-cert: DFN-CERT-2017-0348
```

High (CVSS: 8.1)
NVT: Microsoft Windows Group Policy Elevation of Privilege Vulnerability (3163622)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-072

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Gpapi.dll
File version:     6.1.7600.16385
Vulnerable range:
```

Impact
Successful exploitation will allow an attacker to potentially escalate permissions or perform additional privileged actions on the target machine.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight
An elevation of privilege flaw exists when Microsoft Windows processes group policy updates.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Group Policy Elevation of Privilege Vulnerability (3163622)`
OID:1.3.6.1.4.1.25623.1.0.808162
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3223
url: https://support.microsoft.com/en-us/kb/3159398
url: https://technet.microsoft.com/library/security/MS16-072
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0914
```

High (CVSS: 8.1)
NVT: Microsoft Windows Monthly Rollup (KB4015549)

Summary
This host is missing a monthly rollup according to Microsoft security update KB4015549.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Ole32.dll
File version:     6.1.7601.17514
Vulnerable range:  Less than 6.1.7601.23714
```

Impact
Successful exploitation will allow an attacker to execute code or elevate user privileges, take control of the affected system, and access information from one domain and inject it into another domain.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
This security update includes improvements and resolves the following security vulnerabilities in Windows: scripting engine, Hyper-V, libjpeg image-processing library, Adobe Type Manager Font Driver, Win32K, Microsoft Outlook, Internet Explorer, Graphics Component, Windows kernel-mode drivers and Lightweight Directory Access Protocol.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Monthly Rollup (KB4015549)`
OID:1.3.6.1.4.1.25623.1.0.810851
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2013-6629
cve: CVE-2017-0058
cve: CVE-2017-0155
cve: CVE-2017-0156
cve: CVE-2017-0158
cve: CVE-2017-0163
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-0166
cve: CVE-2017-0168
cve: CVE-2017-0180
cve: CVE-2017-0182
cve: CVE-2017-0183
cve: CVE-2017-0184
cve: CVE-2017-0191
cve: CVE-2017-0192
cve: CVE-2017-0199
cve: CVE-2017-0202
cve: CVE-2017-0210
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4015549
url: http://www.securityfocus.com/bid/63676
url: http://www.securityfocus.com/bid/97462
url: http://www.securityfocus.com/bid/97471
url: http://www.securityfocus.com/bid/97507
url: http://www.securityfocus.com/bid/97455
url: http://www.securityfocus.com/bid/97465
url: http://www.securityfocus.com/bid/97446
url: http://www.securityfocus.com/bid/97418
url: http://www.securityfocus.com/bid/97444
url: http://www.securityfocus.com/bid/97427
url: http://www.securityfocus.com/bid/97428
url: http://www.securityfocus.com/bid/97435
url: http://www.securityfocus.com/bid/97466
url: http://www.securityfocus.com/bid/97452
url: http://www.securityfocus.com/bid/97498
url: http://www.securityfocus.com/bid/97441
url: http://www.securityfocus.com/bid/97512
cert-bund: CB-K17/0622
cert-bund: CB-K17/0621
cert-bund: CB-K17/0620
cert-bund: CB-K17/0616
cert-bund: CB-K15/1514
cert-bund: CB-K14/1569
cert-bund: CB-K14/1048
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0728
cert-bund: CB-K14/0668
cert-bund: CB-K14/0592
cert-bund: CB-K14/0590
cert-bund: CB-K14/0572
cert-bund: CB-K14/0561
cert-bund: CB-K14/0527
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/0467
cert-bund: CB-K14/0455
cert-bund: CB-K14/0442
cert-bund: CB-K14/0283
cert-bund: CB-K14/0231
cert-bund: CB-K14/0061
cert-bund: CB-K14/0002
cert-bund: CB-K13/1067
cert-bund: CB-K13/1039
cert-bund: CB-K13/1021
cert-bund: CB-K13/0981
cert-bund: CB-K13/0918
cert-bund: CB-K13/0731
dfn-cert: DFN-CERT-2017-0643
dfn-cert: DFN-CERT-2017-0642
dfn-cert: DFN-CERT-2017-0638
dfn-cert: DFN-CERT-2017-0637
dfn-cert: DFN-CERT-2013-2129
dfn-cert: DFN-CERT-2013-2106
dfn-cert: DFN-CERT-2013-2049
dfn-cert: DFN-CERT-2013-2046
dfn-cert: DFN-CERT-2013-1995
dfn-cert: DFN-CERT-2013-1934
dfn-cert: DFN-CERT-2013-1729
```

High (CVSS: 8.1)
NVT: Microsoft Windows Monthly Rollup (KB4019264)

Summary
This host is missing a critical security update (monthly rollup) according to Microsoft KB4019264.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Ole32.dll
File version:     6.1.7601.17514
Vulnerable range:  Less than 6.1.7601.23775
```

Impact
Successful exploitation will allow an attacker to execute code or elevate user privileges, take control of the affected system, bypass security restrictions, conduct denial-of-service condition, gain access to potentially sensitive information and spoof content by tricking a user by redirecting the user to a specially crafted website.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

This monthly rollup,

- Addressed issue where applications that use msado15.dll stop working after installing security update 4015550.
- Deprecated SHA-1 Microsoft Edge and Internet Explorer 11 for SSL/TLS Server Authentication.
- Updated Internet Explorer 11's New Tab Page with an integrated newsfeed.
- Includes security updates to Microsoft Graphics Component, Microsoft Windows DNS, Windows COM, Windows Server, Windows kernel, and Internet Explorer.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Monthly Rollup (KB4019264)`

OID:1.3.6.1.4.1.25623.1.0.811114

Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0064
cve: CVE-2017-0077
cve: CVE-2017-0171
cve: CVE-2017-0175
cve: CVE-2017-0190
cve: CVE-2017-0213
cve: CVE-2017-0214
cve: CVE-2017-0220
cve: CVE-2017-0222
cve: CVE-2017-0231
cve: CVE-2017-0242
cve: CVE-2017-0244
cve: CVE-2017-0245
cve: CVE-2017-0246
cve: CVE-2017-0258
cve: CVE-2017-0263
cve: CVE-2017-0267
cve: CVE-2017-0268
cve: CVE-2017-0269
cve: CVE-2017-0270
cve: CVE-2017-0271
cve: CVE-2017-0272
cve: CVE-2017-0273
cve: CVE-2017-0274
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-0275
cve: CVE-2017-0276
cve: CVE-2017-0277
cve: CVE-2017-0278
cve: CVE-2017-0279
cve: CVE-2017-0280
cve: CVE-2017-8552
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4019264
url: http://www.securityfocus.com/bid/98121
url: http://www.securityfocus.com/bid/98114
url: http://www.securityfocus.com/bid/98097
url: http://www.securityfocus.com/bid/98110
url: http://www.securityfocus.com/bid/98298
url: http://www.securityfocus.com/bid/98102
url: http://www.securityfocus.com/bid/98103
url: http://www.securityfocus.com/bid/98111
url: http://www.securityfocus.com/bid/98127
url: http://www.securityfocus.com/bid/98173
url: http://www.securityfocus.com/bid/98275
url: http://www.securityfocus.com/bid/98109
url: http://www.securityfocus.com/bid/98115
url: http://www.securityfocus.com/bid/98108
url: http://www.securityfocus.com/bid/98112
url: http://www.securityfocus.com/bid/98258
url: http://www.securityfocus.com/bid/98259
url: http://www.securityfocus.com/bid/98261
url: http://www.securityfocus.com/bid/98263
url: http://www.securityfocus.com/bid/98264
url: http://www.securityfocus.com/bid/98265
url: http://www.securityfocus.com/bid/98260
url: http://www.securityfocus.com/bid/98274
url: http://www.securityfocus.com/bid/98266
url: http://www.securityfocus.com/bid/98267
url: http://www.securityfocus.com/bid/98268
url: http://www.securityfocus.com/bid/98270
url: http://www.securityfocus.com/bid/98271
url: http://www.securityfocus.com/bid/98272
url: http://www.securityfocus.com/bid/98273
cert-bund: CB-K17/0786
cert-bund: CB-K17/0782
cert-bund: CB-K17/0781
dfn-cert: DFN-CERT-2017-0813
dfn-cert: DFN-CERT-2017-0810
dfn-cert: DFN-CERT-2017-0809
```

High (CVSS: 8.1)
NVT: Microsoft Windows Multiple Vulnerabilities (3124901)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-007.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Advapi32.dl
File version:     6.1.7600.16385
Vulnerable range: Less than 6.1.7601.19091
```

Impact
Successful exploitation will allow an attacker to gain access to the remote host as another user, possibly with elevated privileges and to take complete control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
Multiple flaws are due to:
- A security feature bypass vulnerability exists in Windows Remote Desktop Protocol, that is caused when Windows hosts running RDP services fail to prevent remote logon to accounts that have no passwords set.
- Multiple elevation of privilege vulnerabilities exist when Windows improperly validates input before loading dynamic link library (DLL) files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (3124901)`
OID:1.3.6.1.4.1.25623.1.0.807029
Version used: `2023-11-03T05:05:46Z`

References
`cve: CVE-2016-0014`
`cve: CVE-2016-0015`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-0016
cve: CVE-2016-0018
cve: CVE-2016-0019
cve: CVE-2016-0020
url: https://support.microsoft.com/en-us/kb/3121918
url: https://support.microsoft.com/en-us/kb/3109560
url: https://support.microsoft.com/en-us/kb/3110329
url: https://support.microsoft.com/en-us/kb/3108664
url: https://technet.microsoft.com/library/security/MS16-007
cert-bund: CB-K16/0057
```

High (CVSS: 8.1)
NVT: Microsoft Windows Multiple Vulnerabilities (4013078)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-012.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Gdi32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23688
```

Impact
Successful exploitation will allow an attacker to bypass security, obtain sensitive information, run arbitrary code, cause the affected system to stop responding until it is manually restarted, take control of the affected system. An attacker could then:
- install programs
- view, change, or delete data
- create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2016

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws are due to:

- The Device Guard does not properly validate certain elements of a signed PowerShell script.
- An improper handling of certain requests sent by a malicious SMB server to the client.
- Microsoft Windows fails to properly validate input before loading certain dynamic link library (DLL) files.
- Windows dnsclient fails to properly handle requests.
- A DCOM object in Helppane.exe configured to run as the interactive user fails to properly authenticate the client.
- iSNS Server service fails to properly validate input from the client, leading to an integer overflow.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (4013078)`

OID:1.3.6.1.4.1.25623.1.0.810593

Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-0007
cve: CVE-2017-0016
cve: CVE-2017-0039
cve: CVE-2017-0057
cve: CVE-2017-0100
cve: CVE-2017-0104
url: https://support.microsoft.com/en-us/kb/4013078
url: http://www.securityfocus.com/bid/96018
url: http://www.securityfocus.com/bid/95969
url: http://www.securityfocus.com/bid/96024
url: http://www.securityfocus.com/bid/96695
url: http://www.securityfocus.com/bid/96700
url: http://www.securityfocus.com/bid/96697
url: https://technet.microsoft.com/library/security/MS17-012
url: https://technet.microsoft.com/library/security/MS17-012
cert-bund: CB-K17/0443
cert-bund: CB-K17/0197
dfn-cert: DFN-CERT-2017-0451
dfn-cert: DFN-CERT-2017-0200
```

High (CVSS: 8.1)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4284826)

Summary

This host is missing a critical security update according to Microsoft KB4284826

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable range:  Less than 6.1.7601.24150
File checked:      C:\Windows\system32\appidsvc.dll
File version:      6.1.7601.18741
```

Impact

Successful exploitation will allow an attacker to obtain information to further compromise the user's system, run processes in an elevated context, inject code into a trusted PowerShell process, execute arbitrary code, read privileged data, force the browser to send restricted data, install programs and create a denial of service condition.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to errors,

- When Internet Explorer improperly accesses objects in memory.
- When the Windows kernel improperly handles objects in memory.
- When Windows improperly handles objects in memory.
- When the (Human Interface Device) HID Parser Library driver improperly handles objects in memory.
- When NTFS improperly checks access.
- When Windows Media Foundation improperly handles objects in memory.
- In the way that the scripting engine handles objects in memory in Internet Explorer.
- When the Windows kernel fails to properly handle objects in memory.
- In Windows Domain Name System (DNS) DNSAPI.
- In the way that the Windows Code Integrity Module performs hashing.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4284826)`

OID:1.3.6.1.4.1.25623.1.0.813533

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2018-0978
cve: CVE-2018-1036
cve: CVE-2018-1040
cve: CVE-2018-8169
cve: CVE-2018-8205
cve: CVE-2018-8207
cve: CVE-2018-8224
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-8225
cve: CVE-2018-8249
cve: CVE-2018-8251
cve: CVE-2018-8267
url: https://support.microsoft.com/en-us/help/4284826
cert-bund: CB-K18/0726
cert-bund: CB-K18/0724
dfn-cert: DFN-CERT-2018-1141
dfn-cert: DFN-CERT-2018-1137
```

High (CVSS: 8.1)
NVT: Microsoft Edge and Internet Explorer Type Confusion Remote Code Execution Vulnerability

Summary
Microsoft Edge or Internet Explorer is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: 11.0.9600.18538 and prior
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code in the context of the currently logged-in user. Failed attacks will cause denial of service conditions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012R2
- Microsoft Windows 10 Version 1511, 1607 x32/x64
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1

Vulnerability Insight
The flaw exists due to a type confusion issue in the 'Layout::MultiColumnBoxBuilder::HandleColumnBreakOnColumnSpanningElement' function in mshtml.dll.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Microsoft Edge and Internet Explorer Type Confusion Remote Code Execution Vulne.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.810577
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0037
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://bugs.chromium.org/p/project-zero/issues/detail?id=1011
url: http://www.securityfocus.com/bid/96088
url: https://www.exploit-db.com/exploits/41454
url: http://securitytracker.com/id/1037906
url: https://technet.microsoft.com/library/security/MS17-007
url: https://technet.microsoft.com/library/security/MS17-006
cert-bund: CB-K17/0439
cert-bund: CB-K17/0436
cert-bund: CB-K17/0338
dfn-cert: DFN-CERT-2017-0450
dfn-cert: DFN-CERT-2017-0444
dfn-cert: DFN-CERT-2017-0348
```

High (CVSS: 8.1)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4592471)

Summary
This host is missing a critical security update according to Microsoft KB4592471

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24563
File checked:      C:\Windows\system32\Localspl.dll
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to elevate privileges and disclose sensitive information.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to:

- An error in the Backup Engine allows a local authenticated malicious user to gain elevated privileges on the system.
- An error in Kerberos Security Feature.
- An error in the GDI+ component.
- An error in the SMBv2 component. For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4592471)`

OID:1.3.6.1.4.1.25623.1.0.817545

Version used: `2024-06-26T05:05:39Z`

References

```
cve: CVE-2020-16958
cve: CVE-2020-16959
cve: CVE-2020-16960
cve: CVE-2020-16961
cve: CVE-2020-16962
cve: CVE-2020-16963
cve: CVE-2020-16964
cve: CVE-2020-17049
cve: CVE-2020-17098
cve: CVE-2020-17140
url: https://support.microsoft.com/en-us/help/4592471
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2022-2280
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1126
cert-bund: CB-K20/1214
cert-bund: CB-K20/1109
dfn-cert: DFN-CERT-2024-0078
dfn-cert: DFN-CERT-2023-1053
dfn-cert: DFN-CERT-2022-1686
dfn-cert: DFN-CERT-2022-0332
dfn-cert: DFN-CERT-2020-2669
dfn-cert: DFN-CERT-2020-2464
```

High (CVSS: 8.1)

NVT: Microsoft .NET Framework Multiple Vulnerabilities (KB4338417)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing an important security update according to Microsoft KB4338417

Vulnerability Detection Result

```
Vulnerable range:   4.0.30319.30000 - 4.0.30319.36449
File checked:       C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.Identi
↪tyModel.dll
File version:       4.0.30319.34209
```

Impact

Successful exploitation will allow an attacker to gain elevated privileges, bypass security restrictions and take control of an affected system allowing to install programs or view data, change data, delete data or create new accounts with full user rights.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 4.5.2 for Microsoft Windows 7 SP1, Server 2008 R2 SP1, and Microsoft Windows Server 2008.

Vulnerability Insight

Multiple flaws exist due to:

- An error when Microsoft .NET Framework components do not correctly validate certificates.
- An error in the way how .NET Framework activates COM objects.
- An error when the Microsoft .NET Framework fails to validate input properly.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Multiple Vulnerabilities (KB4338417)`

OID:1.3.6.1.4.1.25623.1.0.813485

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2018-8356
cve: CVE-2018-8284
cve: CVE-2018-8202
url: https://support.microsoft.com/en-us/help/4338417
cert-bund: CB-K18/0774
dfn-cert: DFN-CERT-2018-1345
dfn-cert: DFN-CERT-2018-1344
```

High (CVSS: 7.8)
NVT: Microsoft Graphics Component Multiple Vulnerabilities (4013075)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-013.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23677
```

Impact
Successful exploitation will allow an attacker to perform remote code execution, gain access to potentially sensitive information and gain elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x86/x64
- Microsoft Windows XP SP2 x64 / SP3 x86
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10/1511/1607 x32/x64
- Microsoft Windows Server 2012/2012R2/2016
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to
- The way the Windows Graphics Device Interface (GDI) handles objects in memory.
- The Windows GDI component improperly discloses the contents of its memory.
- The way that the Color Management Module (ICM32.dll) handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Graphics Component Multiple Vulnerabilities (4013075)`
OID:1.3.6.1.4.1.25623.1.0.810811
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2017-0001
cve: CVE-2017-0005
cve: CVE-2017-0025
cve: CVE-2017-0047
cve: CVE-2017-0060
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2017-0062
cve: CVE-2017-0073
cve: CVE-2017-0061
cve: CVE-2017-0063
cve: CVE-2017-0038
cve: CVE-2017-0108
cve: CVE-2017-0014
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013075
url: https://technet.microsoft.com/library/security/MS17-013
cert-bund: CB-K17/0443
cert-bund: CB-K17/0441
dfn-cert: DFN-CERT-2017-0454
dfn-cert: DFN-CERT-2017-0451
```

High (CVSS: 7.8)
NVT: Microsoft .NET Framework Multiple Vulnerabilities (KB4579977)

Summary
This host is missing a critical security update according to Microsoft KB4579977

Vulnerability Detection Result

```
Vulnerable range:   4.0.30319.30000 - 4.0.30319.36683
File checked:       C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.data.d
↪ll
File version:       4.0.30319.34209
```

Impact
Successful exploitation will allow an attacker to gain access to sensitive information and run arbitrary code in the context of the process responsible for deserialization of the XML content.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight
Multiple flaws exist due to:
- An error in .NET Framework when the software fails to check the source markup of XML file input.
- An error when the .NET Framework improperly handles objects in memory.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Multiple Vulnerabilities (KB4579977)`
OID:1.3.6.1.4.1.25623.1.0.817393
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2020-1147
cve: CVE-2020-16937
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4579977
cert-bund: CB-K20/0983
cert-bund: CB-K20/0704
cert-bund: CB-K20/0694
dfn-cert: DFN-CERT-2020-2236
dfn-cert: DFN-CERT-2020-1522
dfn-cert: DFN-CERT-2020-1521
dfn-cert: DFN-CERT-2020-1516
```

High (CVSS: 7.8)
NVT: Windows IExpress Untrusted Search Path Vulnerability

Summary

This host has IExpress bundled with Microsoft Windows and is prone to an untrusted search path vulnerability.

Vulnerability Detection Result

```
Fixed version:     Workaround
File checked:      C:\Windows\system32\IEXPRESS.EXE
File version:      8.0.7600.16385
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code with the privilege of the user invoking a vulnerable self-extracting archive file.

Solution:

Solution type: Workaround

As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory and make sure there are no suspicious files in the directory where self-extracting archive files are saved.

Affected Software/OS

IExpress bundled with Microsoft Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The flaw exists due to an untrusted search path error in self-extracting archive files created by IExpress bundled with Microsoft Windows.

Vulnerability Detection Method

Check for the presence of IExpress (IEXPRESS.EXE).

Details: `Windows IExpress Untrusted Search Path Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.813808

Version used: `2023-07-20T05:05:18Z`

References

```
cve: CVE-2018-0598
url: http://jvn.jp/en/jp/JVN72748502/index.html
url: https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-
↪vulnerability
```

High (CVSS: 7.8)

NVT: Microsoft Remote Desktop Protocol Security Advisory (2861855)

Summary

This host is missing an important security update according to Microsoft advisory (2861855).

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to bypass the security.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

The flaw is due to security issue in Network-level Authentication (NLA) method in Remote Desktop Sessions.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Microsoft Remote Desktop Protocol Security Advisory (2861855)`
OID:1.3.6.1.4.1.25623.1.0.803867
Version used: `2021-08-05T12:20:54Z`

References
url: https://support.microsoft.com/kb/2861855
url: https://technet.microsoft.com/en-us/security/advisory/2861855

High (CVSS: 7.8)
NVT: Microsoft Graphics Component Multiple Vulnerabilities (3164036)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-074.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Gdi32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23452
```

Impact
Successful exploitation will allow an attacker to retrieve information that could lead to an Address Space Layout Randomization (ASLR) bypass, and to run processes in an elevated context, and execute arbitrary code and take control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
Multiple flaws are due to:
- the Windows Graphics Component (GDI32.dll) fails to properly handle objects in memory.
- the Windows improperly handles objects in memory.
- Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Graphics Component Multiple Vulnerabilities (3164036)`

OID:1.3.6.1.4.1.25623.1.0.808086

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3216
cve: CVE-2016-3219
cve: CVE-2016-3220
url: https://support.microsoft.com/en-us/kb/3164036
url: https://technet.microsoft.com/library/security/MS16-074
cert-bund: CB-K16/0914
```

High (CVSS: 7.8)

NVT: Microsoft Graphics Component Multiple Vulnerabilities (3185848)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS16-106.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23528
```

Impact

Successful exploitation will allow an attacker to run arbitrary code in kernel mode, to retrieve information from a targeted system, also could take control of the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple flaws are due to:
- The way that certain Windows kernel-mode drivers handle objects in memory.
- The way that the Windows Graphics Device Interface handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Graphics Component Multiple Vulnerabilities (3185848)`
OID:1.3.6.1.4.1.25623.1.0.809307
Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-3348
cve: CVE-2016-3349
cve: CVE-2016-3354
cve: CVE-2016-3355
cve: CVE-2016-3356
url: https://support.microsoft.com/en-us/kb/3185911
url: http://www.securityfocus.com/bid/92782
url: http://www.securityfocus.com/bid/92783
url: http://www.securityfocus.com/bid/92784
url: http://www.securityfocus.com/bid/92787
url: https://technet.microsoft.com/library/security/MS16-106
cert-bund: CB-K16/1406
```

High (CVSS: 7.8)
NVT: Microsoft Kernel-Mode Drivers Elevation of Privilege Vulnerabilities (3136082)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-018.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19113
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight

The flaw exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Kernel-Mode Drivers Elevation of Privilege Vulnerabilities (3136082)`

OID:1.3.6.1.4.1.25623.1.0.807242

Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-0048
url: https://support.microsoft.com/en-us/kb/3136082
url: https://technet.microsoft.com/en-us/library/security/MS16-018
cert-bund: CB-K16/0220
```

High (CVSS: 7.8)

NVT: Microsoft Kernel-Mode Drivers Multiple Privilege Elevation Vulnerabilities (3171481)

Summary

This host is missing an important security update according to Microsoft Bulletin MS16-090.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23471
```

Impact

Successful exploitation will allow an attacker to run arbitrary code in kernel mode, and obtain information to further compromise the user's system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight

Multiple flaws exist due to:
- When the Windows kernel-mode driver fails to properly handle objects in memory.
- When the Windows GDI component improperly discloses kernel memory addresses.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Kernel-Mode Drivers Multiple Privilege Elevation Vulnerabilities (317.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.808577

Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2016-3249
cve: CVE-2016-3250
cve: CVE-2016-3251
cve: CVE-2016-3252
cve: CVE-2016-3254
cve: CVE-2016-3286
url: https://support.microsoft.com/en-us/kb/3171481
url: http://www.securityfocus.com/bid/91597
url: http://www.securityfocus.com/bid/91613
url: http://www.securityfocus.com/bid/91600
url: http://www.securityfocus.com/bid/91614
url: http://www.securityfocus.com/bid/91615
url: http://www.securityfocus.com/bid/91616
url: https://technet.microsoft.com/en-us/library/security/MS16-090
url: https://technet.microsoft.com/library/security/MS16-090
cert-bund: CB-K16/1057
```

High (CVSS: 7.8)
NVT: Microsoft Kernel-Mode Drivers Multiple Privilege Elevation Vulnerabilities (3178466)

Summary

This host is missing an important security update according to Microsoft Bulletin MS16-098.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable range: Less than 6.1.7601.23497
```

Impact

Successful exploitation will allow an attacker to run arbitrary code in kernel mode, and obtain information to further compromise the user's system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight

Multiple flaws exist when the Windows kernel-mode driver fails to properly handle objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Kernel-Mode Drivers Multiple Privilege Elevation Vulnerabilities (317.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.808784

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3308
cve: CVE-2016-3309
cve: CVE-2016-3310
cve: CVE-2016-3311
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3178466
url: http://www.securityfocus.com/bid/92295
url: http://www.securityfocus.com/bid/92297
url: http://www.securityfocus.com/bid/92298
url: http://www.securityfocus.com/bid/92299
url: https://technet.microsoft.com/en-us/library/security/MS16-098
url: https://technet.microsoft.com/library/security/MS16-098
cert-bund: CB-K16/1216
```

High (CVSS: 7.8)
NVT: Microsoft Kernel-Mode Drivers Privilege Elevation Vulnerabilities (3143145)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-034.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19145
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight
The flaws exist in Windows when the Windows kernel-mode driver fails to properly handle objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Kernel-Mode Drivers Privilege Elevation Vulnerabilities (3143145)`
OID:1.3.6.1.4.1.25623.1.0.807308
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0093
cve: CVE-2016-0094
cve: CVE-2016-0095
cve: CVE-2016-0096
url: https://support.microsoft.com/en-us/kb/3143145
url: https://technet.microsoft.com/en-us/library/security/MS16-034
cert-bund: CB-K16/0383
```

High (CVSS: 7.8)
NVT: Microsoft Kernel-Mode Drivers Privilege Elevation Vulnerabilities (3158222)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-062.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23418
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode, and to take control over the affected system, also could retrieve the memory address of a kernel object.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight
Multiple flaws exist due to:
- When the Windows kernel-mode driver fails to properly handle objects in memory and incorrectly maps kernel memory
- When the DirectX Graphics kernel subsystem (dxgkrnl.sys) improperly handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Kernel-Mode Drivers Privilege Elevation Vulnerabilities (3158222)`
OID:1.3.6.1.4.1.25623.1.0.808018
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0171
cve: CVE-2016-0173
cve: CVE-2016-0174
cve: CVE-2016-0196
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2016-0175
cve: CVE-2016-0176
cve: CVE-2016-0197
url: https://support.microsoft.com/en-us/kb/3158222
url: https://technet.microsoft.com/en-us/library/security/MS16-062
url: https://technet.microsoft.com/library/security/MS16-062
cert-bund: CB-K16/0701
```

High (CVSS: 7.8)
NVT: Microsoft Kernel-Mode Drivers Privilege Elevation Vulnerabilities (3164028)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-073.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23452
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode, and potentially disclose contents of memory to which they should not have access.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight
Multiple flaws exist due to:
- When the Windows kernel-mode driver fails to properly handle objects in memory.
- When the Windows Virtual PCI (VPCI) virtual service provider (VSP) fails to properly handle uninitialized memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Microsoft Kernel-Mode Drivers Privilege Elevation Vulnerabilities (3164028)`
OID:1.3.6.1.4.1.25623.1.0.808084
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2016-3218
cve: CVE-2016-3221
cve: CVE-2016-3232
url: https://support.microsoft.com/en-us/kb/3164028
url: https://technet.microsoft.com/en-us/library/security/MS16-073
url: https://technet.microsoft.com/library/security/MS16-073
cert-bund: CB-K16/0914
```

High (CVSS: 7.8)
NVT: Microsoft .NET Framework 4.5.2 Security Feature Bypass And DoS Vulnerabilities

Summary
This host is missing an important security update according to Microsoft KB4096495

Vulnerability Detection Result

```
Vulnerable range:   4.0.30319.30000 - 4.0.30319.36439
File checked:       C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll
File version:       4.0.30319.34209
```

Impact
Successful exploitation will allow an attacker to cause a denial of service and circumvent a User Mode Code Integrity (UMCI) policy on the machine.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An error when .NET and .NET Core improperly process XML documents.
- An error In .Net Framework which could allow an attacker to bypass Device Guard.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework 4.5.2 Security Feature Bypass And DoS Vulnerabilities`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.813184
Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-0765
cve: CVE-2018-1039
url: https://support.microsoft.com/en-us/help/4096495
cert-bund: CB-K18/0656
dfn-cert: DFN-CERT-2018-0870
```

High (CVSS: 7.8)
NVT: Microsoft .NET Framework Multiple Vulnerabilities (KB4570506)

Summary

This host is missing an important security update according to Microsoft KB4570506

Vulnerability Detection Result

```
Vulnerable range:  4.0 - 4.0.30319.36659
File checked:      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Webengine.dll
File version:      4.0.30319.34209
```

Impact

Successful exploitation will allow an attacker to gain access to restricted files and take control of an affected system

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight

Multiple flaws exist due to

- An error when ASP.NET or .NET web applications running on IIS improperly allow access to cached files.
- An error when Microsoft .NET Framework processes input.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Multiple Vulnerabilities (KB4570506)`
OID:1.3.6.1.4.1.25623.1.0.817320
Version used: `2021-08-11T08:56:08Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2020-1476
cve: CVE-2020-1046
url: https://support.microsoft.com/en-us/help/4570506
cert-bund: CB-K20/0811
dfn-cert: DFN-CERT-2020-1773
```

High (CVSS: 7.8)
NVT: Microsoft .NET Framework Remote Code Execution Vulnerability (KB4014981)

Summary

This host is missing a critical security update according to Microsoft Security Updates KB4014981

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\system.manage
↪ment.dll
File version:     4.0.30319.34209
Vulnerable range: 4.0.30319.30000 - 4.0.30319.36387
```

Impact

Successful exploitation will allow remote attackers to take control of an affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6/4.6.1
- Microsoft .NET Framework 4.6.2

Vulnerability Insight

Flaw exists as .NET Framework fails to properly validate input before loading libraries.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Remote Code Execution Vulnerability (KB4014981)`

OID:1.3.6.1.4.1.25623.1.0.810861

Version used: `2024-03-05T05:05:54Z`

References

```
cve: CVE-2017-0160
url: https://support.microsoft.com/en-us/help/4014981
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0617
dfn-cert: DFN-CERT-2017-0639
```

High (CVSS: 7.8)
NVT: Microsoft .NET Framework Remote Code Execution Vulnerability (KB4014984)

Summary
This host is missing a critical security update according to Microsoft Security Updates KB4014984

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\system.manage
↪ment.dll
File version:     4.0.30319.34209
Vulnerable range: 4.0.30319.30000 - 4.0.30319.36387
```

Impact
Successful exploitation will allow remote attackers to take control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6

Vulnerability Insight
Flaw exists as .NET Framework fails to properly validate input before loading libraries.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Remote Code Execution Vulnerability (KB4014984)`
OID:1.3.6.1.4.1.25623.1.0.810868
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0160
url: https://support.microsoft.com/en-us/help/4014984
cert-bund: CB-K17/0617
dfn-cert: DFN-CERT-2017-0639
```

High (CVSS: 7.8)
NVT: Microsoft .NET Framework Remote Code Execution Vulnerability (KB4566517)

Summary
This host is missing a critical security update according to Microsoft KB4566517

Vulnerability Detection Result

```
Vulnerable range:   4.0 - 4.0.30319.36644
File checked:       C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.data.d
↪ll
File version:       4.0.30319.34209
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in the context of the process responsible for deserialization of the XML content.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight
The flaw exists due to an error in .NET Framework when the software fails to check the source markup of XML file input.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Remote Code Execution Vulnerability (KB4566517)`
OID:1.3.6.1.4.1.25623.1.0.817308
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2020-1147
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4566517
cert-bund: CB-K20/0704
cert-bund: CB-K20/0694
dfn-cert: DFN-CERT-2020-1522
dfn-cert: DFN-CERT-2020-1521
dfn-cert: DFN-CERT-2020-1516
```

High (CVSS: 7.8)
NVT: Microsoft Video Control Remote Code Execution Vulnerability (3199151)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-131.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23584
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in the context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64

Vulnerability Insight
The flaw exists due to microsoft video control fails to properly handle objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Video Control Remote Code Execution Vulnerability (3199151)`
OID:1.3.6.1.4.1.25623.1.0.809800
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-7248
url: https://support.microsoft.com/en-us/kb/3193706
url: http://www.securityfocus.com/bid/94028
url: https://technet.microsoft.com/en-us/library/security/MS16-131
url: https://technet.microsoft.com/library/security/MS16-131
cert-bund: CB-K16/1747
```

High (CVSS: 7.8)
NVT: Microsoft Windows Authentication Methods Multiple Vulnerabilities (3199173)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-137.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23584
```

Impact
Successful exploitation will allow a locally-authenticated to read sensitive information on the target system, cause the target system to become non-responsive and elevate their permissions from unprivileged to administrator which thereby allows him/her to install programs, view, change or delete data, or create new accounts.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Multiple flaws exist due to:
- The windows Virtual Secure Mode improperly handles objects in memory.
- A denial of service vulnerability in the Local Security Authority Subsystem Service (LSASS).
- The windows fails to properly handle NTLM password change requests.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Authentication Methods Multiple Vulnerabilities (3199173)`
OID:1.3.6.1.4.1.25623.1.0.809093
Version used: `2023-07-20T05:05:17Z`

References
`cve: CVE-2016-7238`
`cve: CVE-2016-7237`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-7220
url: https://support.microsoft.com/en-us/kb/3199173
url: http://www.securityfocus.com/bid/92835
url: https://technet.microsoft.com/en-us/library/security/ms16-137
cert-bund: CB-K16/1747
```

High (CVSS: 7.8)
NVT: Microsoft Windows Common Log File System Driver Elevation of Privilege Vulnerability (3193706)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-134.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\clfs.sys
File version:     6.1.7600.16385
Vulnerable range: Less than 6.1.7601.23572
```

Impact
Successful exploitation will allow an attacker to run processes in an elevated context.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64

Vulnerability Insight
The flaw exists due to windows common log file system (CLFS) driver improperly handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Common Log File System Driver Elevation of Privilege Vulnerab.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809801

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0026
cve: CVE-2016-3332
cve: CVE-2016-3333
cve: CVE-2016-3334
cve: CVE-2016-3335
cve: CVE-2016-3338
cve: CVE-2016-3340
cve: CVE-2016-3342
cve: CVE-2016-3343
cve: CVE-2016-7184
url: https://support.microsoft.com/en-us/kb/3193706
url: http://www.securityfocus.com/bid/93998
url: http://www.securityfocus.com/bid/94008
url: http://www.securityfocus.com/bid/94009
url: http://www.securityfocus.com/bid/94012
url: http://www.securityfocus.com/bid/94011
url: http://www.securityfocus.com/bid/94014
url: http://www.securityfocus.com/bid/94010
url: http://www.securityfocus.com/bid/94013
url: http://www.securityfocus.com/bid/94007
url: http://www.securityfocus.com/bid/94015
url: https://technet.microsoft.com/en-us/library/security/MS16-134
cert-bund: CB-K16/1747
```

High (CVSS: 7.8)
NVT: Microsoft Windows ICMPv6 Packet Denial of Service Vulnerability (2868623)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-065.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to cause denial of service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2012
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
Flaw is due to an error within the TCP/IP stack when handling ICMPv6 packets.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows ICMPv6 Packet Denial of Service Vulnerability (2868623)`
OID:1.3.6.1.4.1.25623.1.0.903316
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2013-3183
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-065
url: http://www.securityfocus.com/bid/61666
dfn-cert: DFN-CERT-2013-1468
```

High (CVSS: 7.8)
NVT: Microsoft Windows Information Disclosure And Elevation of Privilege Vulnerabilities (3205655)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-149.

Vulnerability Detection Result
```
File checked:     C:\Windows\System32\msi.dll
File version:     5.0.7601.17514
Vulnerable range: Less than 5.0.7601.23593
```

Impact
Successful exploitation will allow attackers to obtain information to further compromise the user's system, run arbitrary code with elevated system privileges. An attacker could then install programs, view, change, or delete data or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight

Multiple flaws exist due to:

- The windows Crypto driver running in kernel mode improperly handles objects in memory.
- The windows Installer fails to properly sanitize input leading to an insecure library loading behavior.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Information Disclosure And Elevation of Privilege Vulnerabili.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.810238

Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-7219
cve: CVE-2016-7292
url: https://support.microsoft.com/en-us/kb/3205655
url: http://www.securityfocus.com/bid/94768
url: http://www.securityfocus.com/bid/94764
url: https://technet.microsoft.com/en-us/library/security/MS16-149
url: https://technet.microsoft.com/library/security/MS16-149
cert-bund: CB-K16/1959
```

High (CVSS: 7.8)
NVT: Microsoft Windows Kernel Elevation of Privilege Vulnerability (KB4100480)

Summary

This host is missing a critical security update according to Microsoft KB4100480

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24059
File checked:       C:\Windows\system32\kernel32.dll
File version:       6.1.7601.17514
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow an attacker to run arbitrary code in kernel mode which will empower them to install programs, view, change, delete data or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
The flaw exists due to Windows kernel failing to properly handle objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel Elevation of Privilege Vulnerability (KB4100480)`
OID:1.3.6.1.4.1.25623.1.0.812848
Version used: `2023-07-20T05:05:17Z`

References
```
cve: CVE-2018-1038
url: https://support.microsoft.com/en-us/help/4100480
url: http://www.securityfocus.com/bid/103549
cert-bund: CB-K18/0558
dfn-cert: DFN-CERT-2018-0609
```

High (CVSS: 7.8)
NVT: Microsoft Windows Kernel Mode Drivers Multiple Vulnerabilities (3205651)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-151

Vulnerability Detection Result
```
File checked:     C:\Windows\system32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23591
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode and run processes in an elevated context.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Multiple flaws exist due to:
- The Windows Graphics Component improperly handles objects in memory.
- The Windows kernel-mode driver fails to properly handle objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel Mode Drivers Multiple Vulnerabilities (3205651)`
OID:1.3.6.1.4.1.25623.1.0.810308
Version used: `2023-07-21T05:05:22Z`

References
```
cve: CVE-2016-7259
cve: CVE-2016-7260
url: https://support.microsoft.com/en-us/kb/3205651
url: http://www.securityfocus.com/bid/94785
url: http://www.securityfocus.com/bid/94771
url: https://technet.microsoft.com/en-us/library/security/ms16-151
cert-bund: CB-K16/1959
```

High (CVSS: 7.8)
NVT: Microsoft Windows Kernel Multiple Vulnerabilities (3186973)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-111

Vulnerability Detection Result
```
File checked:     C:\Windows\system32\Ntoskrnl.exe
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.23539
```

. . . continues on next page . . .

... continued from previous page ...

Impact

Successful exploitation will allow local attackers to hijack the session of another user and to gain access to information that is not intended for the user and to impersonate processes, interject cross-process communication, or interrupt sslystem functionality.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight

Multiple flaws exist due to:

- The kernel API improperly allows a user to access sensitive registry information.
- The kernel API improperly enforces permissions.
- Windows improperly handles session objects

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel Multiple Vulnerabilities (3186973)`

OID:1.3.6.1.4.1.25623.1.0.809220

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3305
cve: CVE-2016-3306
cve: CVE-2016-3371
cve: CVE-2016-3372
cve: CVE-2016-3373
url: https://support.microsoft.com/en-us/kb/3186973
url: http://www.securityfocus.com/bid/92812
url: http://www.securityfocus.com/bid/92813
url: http://www.securityfocus.com/bid/92814
url: http://www.securityfocus.com/bid/92815
url: http://www.securityfocus.com/bid/92845
url: https://technet.microsoft.com/en-us/library/security/MS16-111
url: https://technet.microsoft.com/library/security/MS16-111
cert-bund: CB-K16/1406
```

High (CVSS: 7.8)
NVT: Microsoft Windows Kernel Privilege Escalation Vulnerability (4013081)

Summary
This host is missing an important security update according to Microsoft Bulletin MS17-017

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23677
```

Impact
Successful exploitation will allow an attacker to gain elevated privileges on a targeted system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2016

Vulnerability Insight
Multiple flaws exist as,
- Windows kernel API enforces permissions.
- Windows Transaction Manager improperly handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel Privilege Escalation Vulnerability (4013081)`
OID:1.3.6.1.4.1.25623.1.0.810814
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0050
cve: CVE-2017-0101
cve: CVE-2017-0102
cve: CVE-2017-0103
cisa: Known Exploited Vulnerability (KEV) catalog
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013081
url: http://www.securityfocus.com/bid/96025
url: http://www.securityfocus.com/bid/96625
url: http://www.securityfocus.com/bid/96627
url: http://www.securityfocus.com/bid/96623
url: https://technet.microsoft.com/en-us/library/security/MS17-017
url: https://technet.microsoft.com/library/security/MS17-017
cert-bund: CB-K17/0443
dfn-cert: DFN-CERT-2017-0451
```

High (CVSS: 7.8)
NVT: Microsoft Windows Kernel-Mode Drivers Multiple Vulnerabilities (3199135)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-135

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\drivers\Bowser.sys
File version:     6.1.7600.16385
Vulnerable range: Less than 6.1.7601.23567
```

Impact
Successful exploitation will allow an attacker to retrieve the memory address of a kernel object, run arbitrary code in kernel mode and to log on to an affected system and runs a specially crafted application that could exploit the vulnerabilities and take control of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Multiple flaws exist due to:
- A kernel Address Space Layout Randomization (ASLR) bypass error.

. . . continues on next page . . .

. . . continued from previous page . . .

- The windows kernel-mode driver fails to properly handle objects in memory.
- The windows bowser.sys kernel-mode driver fails to properly handle objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel-Mode Drivers Multiple Vulnerabilities (3199135)`

OID:1.3.6.1.4.1.25623.1.0.809092

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-7214
cve: CVE-2016-7215
cve: CVE-2016-7218
cve: CVE-2016-7246
cve: CVE-2016-7255
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3199135
url: http://www.securityfocus.com/bid/92835
url: https://technet.microsoft.com/en-us/library/security/ms16-135
cert-bund: CB-K16/1747
```

High (CVSS: 7.8)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (3192892)

Summary

This host is missing an important security update according to Microsoft Bulletin MS16-123.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23545
```

Impact

Successful exploitation will allow an attacker could run arbitrary code in kernel mode. An attacker could then install programs view, change, or delete data, or create new accounts with full user rights, and take control over the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64

Vulnerability Insight

Multiple flaws exist due to:

- The kernel-mode driver fails to properly handle objects in memory.
- The Windows Transaction Manager improperly handles objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (3192.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.809343

Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2016-3266
cve: CVE-2016-3376
cve: CVE-2016-7185
cve: CVE-2016-7211
cve: CVE-2016-3341
url: https://support.microsoft.com/en-us/kb/3192892
url: http://www.securityfocus.com/bid/93384
url: http://www.securityfocus.com/bid/93388
url: http://www.securityfocus.com/bid/93389
url: http://www.securityfocus.com/bid/93391
url: https://technet.microsoft.com/library/security/MS16-123
cert-bund: CB-K16/1582
```

High (CVSS: 7.8)

NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (4013083)

Summary

This host is missing an important security update according to Microsoft Bulletin MS17-018.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Gdi32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23688
```

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow an attacker to run arbitrary code in kernel mode. An attacker could then:
- install programs
- view, change, or delete data
- create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2016

Vulnerability Insight
Multiple flaws exist when the Windows kernel-mode driver fails to properly handle objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (4013.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.810594
Version used: `2023-07-14T16:09:27Z`

References
```
cve: CVE-2017-0024
cve: CVE-2017-0026
cve: CVE-2017-0056
cve: CVE-2017-0078
cve: CVE-2017-0079
cve: CVE-2017-0080
cve: CVE-2017-0081
cve: CVE-2017-0082
url: https://support.microsoft.com/en-us/kb/4013083
url: http://www.securityfocus.com/bid/96029
url: http://www.securityfocus.com/bid/96032
url: http://www.securityfocus.com/bid/96630
```

... continues on next page ...

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/96631
url: http://www.securityfocus.com/bid/96632
url: http://www.securityfocus.com/bid/96633
url: http://www.securityfocus.com/bid/96634
url: http://www.securityfocus.com/bid/96635
url: https://technet.microsoft.com/library/security/MS17-018
url: https://technet.microsoft.com/library/security/MS17-018
cert-bund: CB-K17/0443
dfn-cert: DFN-CERT-2017-0451
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (3134228)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-014.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Ntdll.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19117
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code in kernel mode, to cause denial of service conditions, to bypass authentication and can launch further attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
Multiple flaws are due to:
- Windows kernel improperly handles objects in memory.
- Windows improperly validates input before loading dynamic link library (DLL) files.
- Insufficient validation of input by Microsoft Sync Framework.
- Kerberos fails to check the password change of a user signing into a workstation.

. . . continues on next page . . .

. . . continued from previous page . . .

- A security feature bypass vulnerability exists in Windows Remote Desktop Protocol, that is caused when Windows hosts running RDP services fail to prevent remote logon to accounts that have no passwords set.
- Multiple elevation of privilege vulnerabilities exist when Windows improperly validates input before loading dynamic link library (DLL) files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (3134228)`
OID:1.3.6.1.4.1.25623.1.0.807065
Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-0040
cve: CVE-2016-0041
cve: CVE-2016-0042
cve: CVE-2016-0044
cve: CVE-2016-0049
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3126587
url: https://support.microsoft.com/en-us/kb/3126593
url: https://support.microsoft.com/en-us/kb/3126434
url: https://support.microsoft.com/en-us/kb/3135174
url: https://technet.microsoft.com/library/security/MS16-014
cert-bund: CB-K16/0222
cert-bund: CB-K16/0220
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (3134228)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-014.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Mtxoci.dll
File version:     2001.12.8530.16385
Vulnerable range: 2001.12.8531.19135
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code in kernel mode, to cause denial of service conditions, to bypass authentication and can launch further attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
Multiple flaws are due to:
- Windows kernel improperly handles objects in memory.
- Windows improperly validates input before loading dynamic link library (DLL) files.
- Insufficient validation of input by Microsoft Sync Framework.
- Kerberos fails to check the password change of a user signing into a workstation.
- A security feature bypass vulnerability exists in Windows Remote Desktop Protocol, that is caused when Windows hosts running RDP services fail to prevent remote logon to accounts that have no passwords set.
- Multiple elevation of privilege vulnerabilities exist when Windows improperly validates input before loading dynamic link library (DLL) files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (3134228)`
OID:1.3.6.1.4.1.25623.1.0.807065
Version used: `2023-07-21T05:05:22Z`

References
```
cve: CVE-2016-0040
cve: CVE-2016-0041
cve: CVE-2016-0042
cve: CVE-2016-0044
cve: CVE-2016-0049
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3126587
url: https://support.microsoft.com/en-us/kb/3126593
url: https://support.microsoft.com/en-us/kb/3126434
url: https://support.microsoft.com/en-us/kb/3135174
url: https://technet.microsoft.com/library/security/MS16-014
cert-bund: CB-K16/0222
cert-bund: CB-K16/0220
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (3199172)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-130.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23584
```

Impact
Successful exploitation will allow an attacker to run arbitrary code with elevated system privileges or run a specially crafted application.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64

Vulnerability Insight
Multiple flaws exist due to
- The Windows Input Method Editor (IME) improperly handles DLL loading.
- The Windows Task Scheduler improperly schedule a new task.
- The Windows image file loading functionality does not properly handle malformed image files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (3199172)`
OID:1.3.6.1.4.1.25623.1.0.809465
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2016-7221
cve: CVE-2016-7222
cve: CVE-2016-7212
url: https://support.microsoft.com/en-us/kb/3199172
url: http://www.securityfocus.com/bid/94021
url: http://www.securityfocus.com/bid/94023
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/94027
url: https://technet.microsoft.com/en-us/library/security/MS16-130
url: https://technet.microsoft.com/library/security/MS16-130
cert-bund: CB-K16/1747
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4048957)

Summary
This host is missing a critical security update according to Microsoft KB4048957

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.23915
File checked:      C:\Windows\system32\advapi32.dll
File version:      6.1.7600.16385
```

Impact
Successful exploitation will allow an attacker to read data that was not intended to be disclosed, and obtain information to further compromise the user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist as,
- This security update includes improvements and resolves the following issues: Addressed issue where applications based on the Microsoft JET Database Engine (Microsoft Access 2007 and older or non-Microsoft applications) fail when creating or opening Microsoft Excel .xls files.
- Security updates to Microsoft Windows Search Component, Microsoft Graphics Component, Windows kernel-mode drivers, Windows Media Player, and Windows kernel.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4048957)`
OID:1.3.6.1.4.1.25623.1.0.812149
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-11869
cve: CVE-2017-11768
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-11788
cve: CVE-2017-11880
cve: CVE-2017-11791
cve: CVE-2017-11827
cve: CVE-2017-11834
cve: CVE-2017-11835
cve: CVE-2017-11837
cve: CVE-2017-11838
cve: CVE-2017-11843
cve: CVE-2017-11846
cve: CVE-2017-11847
cve: CVE-2017-11848
cve: CVE-2017-11849
cve: CVE-2017-11851
cve: CVE-2017-11852
cve: CVE-2017-11853
cve: CVE-2017-11855
cve: CVE-2017-11856
cve: CVE-2017-11858
cve: CVE-2017-11831
cve: CVE-2017-11832
url: https://support.microsoft.com/en-us/help/4048957
url: http://www.securityfocus.com/bid/101742
url: http://www.securityfocus.com/bid/101705
url: http://www.securityfocus.com/bid/101711
url: http://www.securityfocus.com/bid/101755
url: http://www.securityfocus.com/bid/101715
url: http://www.securityfocus.com/bid/101703
url: http://www.securityfocus.com/bid/101725
url: http://www.securityfocus.com/bid/101736
url: http://www.securityfocus.com/bid/101722
url: http://www.securityfocus.com/bid/101737
url: http://www.securityfocus.com/bid/101740
url: http://www.securityfocus.com/bid/101741
url: http://www.securityfocus.com/bid/101729
url: http://www.securityfocus.com/bid/101709
url: http://www.securityfocus.com/bid/101762
url: http://www.securityfocus.com/bid/101763
url: http://www.securityfocus.com/bid/101739
url: http://www.securityfocus.com/bid/101764
url: http://www.securityfocus.com/bid/101751
url: http://www.securityfocus.com/bid/101753
url: http://www.securityfocus.com/bid/101716
url: http://www.securityfocus.com/bid/101721
url: http://www.securityfocus.com/bid/101726
cert-bund: CB-K17/1955
cert-bund: CB-K17/1951
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1949
dfn-cert: DFN-CERT-2017-2040
dfn-cert: DFN-CERT-2017-2039
dfn-cert: DFN-CERT-2017-2031
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4056897)

Summary
This host is missing an important security update according to Microsoft KB4056897

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24000
File checked:      C:\Windows\system32\Advapi32.dll
File version:      6.1.7600.16385
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code and take control of an affected system, elevate their user rights, gain access to sensitive data, bypass certain security checks, impersonate processes, interject cross-process communication, interrupt system functionality and conduct bounds check bypass, branch target injection, rogue data cache load.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory.
- An error in the Windows GDI component which improperly discloses kernel memory addresses.
- An error in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to open a specially crafted file over the SMB protocol on the same machine.
- An error in the way that the Windows Kernel API enforces permissions.
- An error in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass.
- An error in the way that the Color Management Module (ICM32.dll) handles objects in memory.
- Multiple errors leading to 'speculative execution side-channel attacks' that affect many modern processors and operating systems including Intel, AMD, and ARM.

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4056897)`
OID:1.3.6.1.4.1.25623.1.0.812384
Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-0741
cve: CVE-2018-0747
cve: CVE-2018-0748
cve: CVE-2018-0749
cve: CVE-2018-0750
cve: CVE-2018-0754
cve: CVE-2018-0788
cve: CVE-2017-5753
cve: CVE-2017-5715
cve: CVE-2017-5754
url: https://support.microsoft.com/en-us/help/4056897
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-0103
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K20/0324
cert-bund: CB-K19/0774
cert-bund: CB-K18/1140
cert-bund: CB-K18/0898
cert-bund: CB-K18/0654
cert-bund: CB-K18/0651
cert-bund: CB-K18/0635
cert-bund: CB-K18/0601
cert-bund: CB-K18/0557
cert-bund: CB-K18/0551
cert-bund: CB-K18/0518
cert-bund: CB-K18/0472
cert-bund: CB-K18/0463
cert-bund: CB-K18/0398
cert-bund: CB-K18/0381
cert-bund: CB-K18/0370
cert-bund: CB-K18/0367
cert-bund: CB-K18/0356
cert-bund: CB-K18/0348
cert-bund: CB-K18/0347
cert-bund: CB-K18/0346
cert-bund: CB-K18/0338
cert-bund: CB-K18/0283
cert-bund: CB-K18/0257
cert-bund: CB-K18/0250
cert-bund: CB-K18/0244
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K18/0207
cert-bund: CB-K18/0184
cert-bund: CB-K18/0177
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0148
cert-bund: CB-K18/0129
cert-bund: CB-K18/0099
cert-bund: CB-K18/0094
cert-bund: CB-K18/0054
cert-bund: CB-K18/0051
cert-bund: CB-K18/0049
cert-bund: CB-K18/0046
cert-bund: CB-K18/0040
cert-bund: CB-K18/0039
cert-bund: CB-K18/0023
cert-bund: CB-K18/0022
cert-bund: CB-K18/0021
cert-bund: CB-K18/0020
cert-bund: CB-K18/0017
cert-bund: CB-K18/0016
cert-bund: CB-K18/0011
cert-bund: CB-K18/0010
cert-bund: CB-K18/0009
cert-bund: CB-K17/2117
cert-bund: CB-K17/2113
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1377
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-0879
dfn-cert: DFN-CERT-2023-0877
dfn-cert: DFN-CERT-2023-0876
dfn-cert: DFN-CERT-2023-0848
dfn-cert: DFN-CERT-2023-0795
dfn-cert: DFN-CERT-2023-0794
dfn-cert: DFN-CERT-2023-0793
dfn-cert: DFN-CERT-2023-0507
dfn-cert: DFN-CERT-2022-0531
dfn-cert: DFN-CERT-2020-1783
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-1987
dfn-cert: DFN-CERT-2019-1985
dfn-cert: DFN-CERT-2019-1837
dfn-cert: DFN-CERT-2019-1415
dfn-cert: DFN-CERT-2019-1235
dfn-cert: DFN-CERT-2019-1150
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0613
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2465
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1819
dfn-cert: DFN-CERT-2018-1794
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1726
dfn-cert: DFN-CERT-2018-1550
dfn-cert: DFN-CERT-2018-1504
dfn-cert: DFN-CERT-2018-1500
dfn-cert: DFN-CERT-2018-1494
dfn-cert: DFN-CERT-2018-1493
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1386
dfn-cert: DFN-CERT-2018-1385
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1108
dfn-cert: DFN-CERT-2018-1032
dfn-cert: DFN-CERT-2018-1008
dfn-cert: DFN-CERT-2018-0991
dfn-cert: DFN-CERT-2018-0988
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0878
dfn-cert: DFN-CERT-2018-0857
dfn-cert: DFN-CERT-2018-0821
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0815
dfn-cert: DFN-CERT-2018-0808
dfn-cert: DFN-CERT-2018-0799
dfn-cert: DFN-CERT-2018-0796
dfn-cert: DFN-CERT-2018-0794
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0728
dfn-cert: DFN-CERT-2018-0682
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0625
dfn-cert: DFN-CERT-2018-0605
dfn-cert: DFN-CERT-2018-0598
dfn-cert: DFN-CERT-2018-0552
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0510
dfn-cert: DFN-CERT-2018-0499
dfn-cert: DFN-CERT-2018-0427
dfn-cert: DFN-CERT-2018-0410
dfn-cert: DFN-CERT-2018-0397
dfn-cert: DFN-CERT-2018-0394
dfn-cert: DFN-CERT-2018-0382
dfn-cert: DFN-CERT-2018-0377
dfn-cert: DFN-CERT-2018-0375
dfn-cert: DFN-CERT-2018-0372
dfn-cert: DFN-CERT-2018-0367
dfn-cert: DFN-CERT-2018-0310
dfn-cert: DFN-CERT-2018-0276
dfn-cert: DFN-CERT-2018-0267
dfn-cert: DFN-CERT-2018-0262
dfn-cert: DFN-CERT-2018-0224
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0194
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0163
dfn-cert: DFN-CERT-2018-0137
dfn-cert: DFN-CERT-2018-0104
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2018-0066
dfn-cert: DFN-CERT-2018-0058
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0053
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0044
dfn-cert: DFN-CERT-2018-0031
dfn-cert: DFN-CERT-2018-0030
dfn-cert: DFN-CERT-2018-0029
dfn-cert: DFN-CERT-2018-0026
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2018-0024
dfn-cert: DFN-CERT-2018-0022
dfn-cert: DFN-CERT-2018-0020
dfn-cert: DFN-CERT-2018-0019
dfn-cert: DFN-CERT-2017-2211
dfn-cert: DFN-CERT-2017-2210
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4074598)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing a critical security update according to Microsoft KB4074598

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24023
File checked:      C:\Windows\system32\Win32k.sys
File version:      6.1.7601.17514
```

Impact

Successful exploitation will allow an attacker who successfully exploited the vulnerability to run arbitrary code in the context of the current user, read data that was not intended to be disclosed, gain the same user rights as the current user, obtain information to further compromise the user's system, spoof content, perform phishing attacks, or otherwise manipulate content of a document.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- The software fails to properly handle objects in memory.
- The Microsoft Windows Embedded OpenType (EOT) font engine fails to properly parse specially crafted embedded fonts.
- The scripting engine improperly handles objects in memory.
- The Windows Common Log File System (CLFS) driver improperly handles objects in memory.
- The VBScript improperly discloses the contents of its memory.
- The Windows Kernel handles objects in memory.
- The Windows kernel fails to properly initialize a memory address.
- Microsoft has deprecated the Document Signing functionality in XPS Viewer.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4074598)`

OID:1.3.6.1.4.1.25623.1.0.812767

Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-0742
cve: CVE-2018-0755
cve: CVE-2018-0757
cve: CVE-2018-0760
cve: CVE-2018-0761
cve: CVE-2018-0810
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2018-0820
cve: CVE-2018-0825
cve: CVE-2018-0829
cve: CVE-2018-0830
cve: CVE-2018-0840
cve: CVE-2018-0842
cve: CVE-2018-0844
cve: CVE-2018-0846
cve: CVE-2018-0847
cve: CVE-2018-0855
cve: CVE-2018-0866
url: https://support.microsoft.com/en-us/help/4074598
cert-bund: CB-K18/0282
cert-bund: CB-K18/0279
cert-bund: CB-K18/0278
cert-bund: CB-K18/0276
dfn-cert: DFN-CERT-2018-0301
dfn-cert: DFN-CERT-2018-0300
dfn-cert: DFN-CERT-2018-0299
dfn-cert: DFN-CERT-2018-0295
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4103718)

Summary
This host is missing a critical security update according to Microsoft KB4103718

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24117
File checked:      C:\Windows\system32\advapi32.dll
File version:      6.1.7600.16385
```

Impact
Successful exploitation will allow attackers to gain the same user rights as the current user, run arbitrary code, disclose sensitive information and run processes in an elevated context and it may lead to further compromise of the system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to:

- Microsoft browsers improperly access objects in memory.
- The Win32k component fails to properly handle objects in memory.
- Windows kernel fails to properly handle objects in memory.
- The VBScript engine improperly handles objects in memory.
- The scripting engine improperly handles objects in memory in Microsoft browsers.
- Windows Common Log File System (CLFS) driver improperly handles objects in memory.
- Chakra improperly discloses the contents of its memory.
- Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system.
- Windows 'its://' protocol handler unnecessarily sends traffic to a remote site in order to determine the zone of a provided URL.
- An error in Credential Security Support Provider protocol (CredSSP).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4103718)`

OID:1.3.6.1.4.1.25623.1.0.813336

Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-0954
cve: CVE-2018-0955
cve: CVE-2018-0959
cve: CVE-2018-1022
cve: CVE-2018-1025
cve: CVE-2018-8114
cve: CVE-2018-8120
cve: CVE-2018-8122
cve: CVE-2018-8124
cve: CVE-2018-8127
cve: CVE-2018-8136
cve: CVE-2018-8145
cve: CVE-2018-8164
cve: CVE-2018-8166
cve: CVE-2018-8167
cve: CVE-2018-8174
cve: CVE-2018-8178
cve: CVE-2018-8897
cve: CVE-2018-0824
cve: CVE-2017-11927
cve: CVE-2018-0886
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4103718
cert-bund: CB-K18/0698
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0662
cert-bund: CB-K18/0660
cert-bund: CB-K18/0659
cert-bund: CB-K18/0657
cert-bund: CB-K18/0654
cert-bund: CB-K18/0653
cert-bund: CB-K18/0652
cert-bund: CB-K18/0630
cert-bund: CB-K18/0461
cert-bund: CB-K17/2149
dfn-cert: DFN-CERT-2020-1810
dfn-cert: DFN-CERT-2019-0142
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2309
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1072
dfn-cert: DFN-CERT-2018-1059
dfn-cert: DFN-CERT-2018-0988
dfn-cert: DFN-CERT-2018-0936
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0928
dfn-cert: DFN-CERT-2018-0914
dfn-cert: DFN-CERT-2018-0896
dfn-cert: DFN-CERT-2018-0895
dfn-cert: DFN-CERT-2018-0890
dfn-cert: DFN-CERT-2018-0889
dfn-cert: DFN-CERT-2018-0888
dfn-cert: DFN-CERT-2018-0887
dfn-cert: DFN-CERT-2018-0886
dfn-cert: DFN-CERT-2018-0885
dfn-cert: DFN-CERT-2018-0884
dfn-cert: DFN-CERT-2018-0883
dfn-cert: DFN-CERT-2018-0882
dfn-cert: DFN-CERT-2018-0881
dfn-cert: DFN-CERT-2018-0878
dfn-cert: DFN-CERT-2018-0874
dfn-cert: DFN-CERT-2018-0873
dfn-cert: DFN-CERT-2018-0871
dfn-cert: DFN-CERT-2018-0869
dfn-cert: DFN-CERT-2018-0868
dfn-cert: DFN-CERT-2018-0865
dfn-cert: DFN-CERT-2018-0785
dfn-cert: DFN-CERT-2018-0493
dfn-cert: DFN-CERT-2017-2253
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4338818)

Summary
This host is missing a critical security update according to Microsoft KB4338818

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24168
File checked:      C:\Windows\system32\Kernel32.dll
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker to bypass security, cause a target system to stop responding, execute arbitrary code in the context of the current user and elevate privileges on an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to errors,
- When Internet Explorer improperly accesses objects in memory.
- When Windows improperly handles File Transfer Protocol (FTP) connections.
- When the scripting engine improperly handles objects in memory in Internet Explorer.
- When Windows kernel-mode driver fails to properly handle objects in memory.
- When Windows Domain Name System (DNS) DNSAPI.dll fails to properly handle DNS responses.
- When Microsoft WordPad improperly handles embedded OLE objects.
- When Windows fails a check, allowing a sandbox escape.
- Involving side channel speculative execution, known as Lazy FP State Restore.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4338818)`
OID:1.3.6.1.4.1.25623.1.0.813645
Version used: `2023-11-03T16:10:08Z`

References
```
cve: CVE-2018-8282
cve: CVE-2018-0949
cve: CVE-2018-8206
cve: CVE-2018-8242
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-8287
cve: CVE-2018-8288
cve: CVE-2018-8291
cve: CVE-2018-8296
cve: CVE-2018-8304
cve: CVE-2018-8307
cve: CVE-2018-8308
cve: CVE-2018-8309
cve: CVE-2018-8314
cve: CVE-2018-3665
url: https://support.microsoft.com/en-us/help/4338818
cert-bund: CB-K19/0271
cert-bund: CB-K18/0778
cert-bund: CB-K18/0774
cert-bund: CB-K18/0773
cert-bund: CB-K18/0772
cert-bund: CB-K18/0765
cert-bund: CB-K18/0730
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1722
dfn-cert: DFN-CERT-2018-1468
dfn-cert: DFN-CERT-2018-1452
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1385
dfn-cert: DFN-CERT-2018-1357
dfn-cert: DFN-CERT-2018-1356
dfn-cert: DFN-CERT-2018-1355
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1351
dfn-cert: DFN-CERT-2018-1349
dfn-cert: DFN-CERT-2018-1346
dfn-cert: DFN-CERT-2018-1332
dfn-cert: DFN-CERT-2018-1293
dfn-cert: DFN-CERT-2018-1290
dfn-cert: DFN-CERT-2018-1279
dfn-cert: DFN-CERT-2018-1270
dfn-cert: DFN-CERT-2018-1260
dfn-cert: DFN-CERT-2018-1228
dfn-cert: DFN-CERT-2018-1206
dfn-cert: DFN-CERT-2018-1205
dfn-cert: DFN-CERT-2018-1190
dfn-cert: DFN-CERT-2018-1170
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1150
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4471318)

Summary
This host is missing a critical security update according to Microsoft KB4471318

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24313
File checked:      C:\Windows\system32\Win32k.sys
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow attackers to run arbitrary code, elevate privileges and obtain information to further compromise the user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1

Vulnerability Insight
Multiple flaws are due to:
- Windows kernel improperly handles objects in memory.
- Internet Explorer VBScript execution policy does not properly restrict VBScript under specific conditions.
- Scripting engine improperly handles objects in memory in Internet Explorer.
- Windows kernel-mode driver fails to properly handle objects in memory.
- Internet Explorer improperly accesses objects in memory.
- Windows GDI component improperly discloses the contents of its memory.
- Windows Domain Name System (DNS) servers when they fail to properly handle requests.
- Windows Win32k component fails to properly handle objects in memory.
- VBScript engine improperly handles objects in memory.
- Remote Procedure Call runtime improperly initializes objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4471318)`
OID:1.3.6.1.4.1.25623.1.0.814619
Version used: `2023-11-03T16:10:08Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2018-8477
cve: CVE-2018-8514
cve: CVE-2018-8611
cve: CVE-2018-8619
cve: CVE-2018-8621
cve: CVE-2018-8622
cve: CVE-2018-8625
cve: CVE-2018-8631
cve: CVE-2018-8639
cve: CVE-2018-8641
cve: CVE-2018-8643
cve: CVE-2018-8595
cve: CVE-2018-8596
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4471318
cert-bund: CB-K18/1171
cert-bund: CB-K18/1166
dfn-cert: DFN-CERT-2018-2523
dfn-cert: DFN-CERT-2018-2520
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4534310)

Summary

This host is missing a critical security update according to Microsoft KB4534310

Vulnerability Detection Result

```
Vulnerable range:  Less than 11.0.9600.19597
File checked:      C:\Windows\system32\Mshtml.dll
File version:      8.0.7601.17514
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code, obtain information to further compromise the user's system, gain elevated privileges and break out of the Edge AppContainer sandbox and run processes in an elevated context.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist in Microsoft Scripting Engine, Windows Input and Composition, Windows Media, Windows Storage and Filesystems, and Windows Server.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4534310)`
OID:1.3.6.1.4.1.25623.1.0.815560
Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2020-0607
cve: CVE-2020-0608
cve: CVE-2020-0611
cve: CVE-2020-0615
cve: CVE-2020-0620
cve: CVE-2020-0625
cve: CVE-2020-0626
cve: CVE-2020-0627
cve: CVE-2020-0628
cve: CVE-2020-0629
cve: CVE-2020-0630
cve: CVE-2020-0631
cve: CVE-2020-0632
cve: CVE-2020-0634
cve: CVE-2020-0635
cve: CVE-2020-0637
cve: CVE-2020-0639
cve: CVE-2020-0640
cve: CVE-2020-0642
cve: CVE-2020-0643
url: https://support.microsoft.com/en-us/help/4534310
cert-bund: CB-K20/0049
cert-bund: CB-K20/0047
dfn-cert: DFN-CERT-2020-0082
dfn-cert: DFN-CERT-2020-0080
```

High (CVSS: 7.8)
NVT: Microsoft Windows Multiple Vulnerabilities (KB5010404)

Summary

This host is missing an important security update according to Microsoft KB5010404

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Vulnerable range:  Less than 6.1.7601.25860
File checked:      C:\Windows\system32\Ntoskrnl.exe
File version:      6.1.7601.18741
```

Impact

Successful exploitation will allow an attacker to elevate privileges, disclose sensitive information, and conduct DoS attacks.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit Systems Service Pack 1

Vulnerability Insight

Multiple flaws exist due to:

- An elevation of privilege vulnerability in Windows Print Spooler.
- An information disclosure vulnerability in Windows Common Log File System Driver.
- An elevation of privilege vulnerability in Windows Common Log File System Driver.

For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB5010404)`

OID:1.3.6.1.4.1.25623.1.0.818968

Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2022-21981
cve: CVE-2022-21985
cve: CVE-2022-21989
cve: CVE-2022-21997
cve: CVE-2022-21998
cve: CVE-2022-21999
cve: CVE-2022-22000
cve: CVE-2022-22710
cve: CVE-2022-22717
cve: CVE-2022-22718
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/5010404
cert-bund: WID-SEC-2022-1174
cert-bund: CB-K22/0160
```

... continues on next page ...

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2022-0306

High (CVSS: 7.8)
NVT: Microsoft Windows Network Policy Server Denial-of-Service Vulnerability (3014029)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-007.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2012/R2

Vulnerability Insight
The flaw is due to an error within the RADIUS implementation related to Internet Authentication Service (IAS) and Network Policy Server (NPS).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Network Policy Server Denial-of-Service Vulnerability (301402.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.805241
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-0015
url: https://support.microsoft.com/kb/3014029
url: http://www.securityfocus.com/bid/71933
url: https://technet.microsoft.com/library/security/MS15-007
cert-bund: CB-K15/0038
dfn-cert: DFN-CERT-2015-0036
```

High (CVSS: 7.8)
NVT: Microsoft Windows OLE Remote Code Execution Vulnerability (3146706)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-044.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Ole32.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23392
```

Impact
Successful exploitation will allow attackers to execute malicious code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2

Vulnerability Insight
The flaw is due to Microsoft Windows OLE fails to properly validate user input.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows OLE Remote Code Execution Vulnerability (3146706)`
OID:1.3.6.1.4.1.25623.1.0.807789
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0153
url: https://support.microsoft.com/en-us/kb/3146706
url: https://support.microsoft.com/en-us/kb/2919355
url: https://technet.microsoft.com/en-us/library/security/MS16-044
cert-bund: CB-K16/0546
```

High (CVSS: 7.8)
NVT: Microsoft Windows Privilege Elevation Vulnerabilities (3124605)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-008

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Ntoskrnl.exe
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.19110
```

Impact
Successful exploitation will allow an authenticated user to execute code with elevated privileges that would allow them to install programs.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 10 x32/x64

Vulnerability Insight
Multiple flaws are due to improper validation of reparse points being set by sandbox applications

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Privilege Elevation Vulnerabilities (3124605)`
OID:1.3.6.1.4.1.25623.1.0.806818
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2016-0006
cve: CVE-2016-0007
url: https://support.microsoft.com/en-us/kb/3124605
url: https://support.microsoft.com/en-us/kb/3121212
url: https://technet.microsoft.com/library/security/MS16-008
cert-bund: CB-K16/0057
```

High (CVSS: 7.8)
NVT: Microsoft Windows Privilege Elevation Vulnerability (3140410)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-031

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Ntoskrnl.exe
File version:     6.1.7601.18741
Vulnerable range:
```

Impact
Successful exploitation will allow an attacker to run arbitrary code as system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1

Vulnerability Insight
The flaw is due to an imporper sanitization of handles in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Privilege Elevation Vulnerability (3140410)`
OID:1.3.6.1.4.1.25623.1.0.807467
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0087
url: https://support.microsoft.com/en-us/kb/3140410
url: https://technet.microsoft.com/en-us/library/security/MS16-031
url: https://technet.microsoft.com/library/security/MS16-031
cert-bund: CB-K16/0383
```

High (CVSS: 7.8)
NVT: Microsoft Windows Privilege Elevation Vulnerability (3154846)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-060

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Ntoskrnl.exe
File version:     6.1.7601.18741
Vulnerable range:
```

Impact

Successful exploitation will allow an attacker to elevate the privilege if an attacker logs on to an affected system and runs a specially crafted application.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight

The flaw exists when the Windows kernel fails to properly handle parsing of certain symbolic links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Privilege Elevation Vulnerability (3154846)`

OID:1.3.6.1.4.1.25623.1.0.807324

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0180
url: https://support.microsoft.com/en-us/kb/3154846
url: https://support.microsoft.com/en-us/kb/3153171
url: https://technet.microsoft.com/en-us/library/security/MS16-060
url: https://technet.microsoft.com/library/security/MS16-060
cert-bund: CB-K16/0701
```

High (CVSS: 7.8)

NVT: Microsoft Windows Privilege Escalation Vulnerabilities (3178465)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing an important security update according to Microsoft Bulletin MS16-101.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Lsasrv.dll
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.23497
```

Impact

Successful exploitation will allow attackers to bypass certain security restrictions and perform unauthorized actions by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight

Multiple flaws are due to:

- An elevation of privilege vulnerability exists when Windows Netlogon improperly establishes a secure communications channel to a domain controller.
- An elevation of privilege vulnerability exists in Windows when Kerberos improperly handles a password change request and falls back to NT LAN Manager (NTLM) Authentication Protocol as the default authentication protocol.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Privilege Escalation Vulnerabilities (3178465)`

OID:1.3.6.1.4.1.25623.1.0.808291

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3237
cve: CVE-2016-3300
url: https://support.microsoft.com/en-us/kb/3167679
url: http://www.securityfocus.com/bid/92290
url: http://www.securityfocus.com/bid/92296
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://support.microsoft.com/en-us/kb/3177108
url: https://technet.microsoft.com/library/security/MS16-101
cert-bund: CB-K16/1216
```

High (CVSS: 7.8)
NVT: Microsoft Windows Secondary Logon Privilege Elevation Vulnerability (3143141)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-032.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Seclogon.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19148
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight
The flaw exists in Windows when the Secondary Logon Service fails to properly manage request handles in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Secondary Logon Privilege Elevation Vulnerability (3143141)`
OID:1.3.6.1.4.1.25623.1.0.807309
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0099
cisa: Known Exploited Vulnerability (KEV) catalog
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3143141
url: https://technet.microsoft.com/en-us/library/security/MS16-032
url: https://technet.microsoft.com/en-us/library/security/MS16-034
cert-bund: CB-K16/0383
```

High (CVSS: 7.8)
NVT: Microsoft Windows SMB Server Elevation of Privilege Vulnerability (3164038)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-075.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\drivers\mrxsmb10.sys
File version:     6.1.7601.17514
Vulnerable range:
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code with elevated permissions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight
An elevation of privilege flaw exists in the Microsoft Server Message Block (SMB) when an attacker forwards an authentication request intended for another service running on the same machine.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows SMB Server Elevation of Privilege Vulnerability (3164038)`
OID:1.3.6.1.4.1.25623.1.0.807340
Version used: `2023-07-20T05:05:17Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2016-3225
url: https://support.microsoft.com/en-us/kb/3164038
url: https://technet.microsoft.com/library/security/MS16-075
cert-bund: CB-K16/0914
```

High (CVSS: 7.8)
NVT: Microsoft Windows TCP/IP Denial of Service Vulnerability (2790655)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-018.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow attackers to exhaust the non-paged pool and render the system unusable or trigger a restart.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

The flaw is due to an error within the TCP/IP stack, which remains in TCP FIN_WAIT_2 state after receiving an ACK to the FIN packet when handling a tear down sequence.

Vulnerability Detection Method

Details: `Microsoft Windows TCP/IP Denial of Service Vulnerability (2790655)`
OID:1.3.6.1.4.1.25623.1.0.902945
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-0075
url: http://support.microsoft.com/kb/2790655
url: http://www.securityfocus.com/bid/57858
url: http://www.securitytracker.com/id/1028128
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪13-018
dfn-cert: DFN-CERT-2013-0293
```

High (CVSS: 7.8)
NVT: Windows Modules Installer Elevation of Privilege Vulnerability (KB4565354)

Summary
This host is missing an important security update according to Microsoft KB4565354

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.24557
File checked:      C:\Windows\system32\Ntoskrnl.exe
File version:      6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to gain elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
The flaw exists due to Windows Modules Installer fails to properly handle file operations.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Windows Modules Installer Elevation of Privilege Vulnerability (KB4565354)
OID:1.3.6.1.4.1.25623.1.0.817234
Version used: 2021-08-11T08:56:08Z

References

```
cve: CVE-2020-1346
url: https://support.microsoft.com/en-us/help/4565354
cert-bund: CB-K20/0692
dfn-cert: DFN-CERT-2020-1515
```

High (CVSS: 7.6)
NVT: Microsoft WinVerifyTrust Signature Validation Vulnerability (2893294)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing a critical security update according to Microsoft Bulletin MS13-098.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to execute arbitrary code or cause a denial of service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight
Flaw is due to WinVerifyTrust function which does not properly handles the Windows Authenticode signature verification for portable executable(PE) files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft WinVerifyTrust Signature Validation Vulnerability (2893294)`
OID:1.3.6.1.4.1.25623.1.0.903228
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2013-3900
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://support.microsoft.com/kb/2893294
url: http://www.securityfocus.com/bid/64079
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-098
cert-bund: CB-K13/1027
dfn-cert: DFN-CERT-2013-2048
```

High (CVSS: 7.6)
NVT: Microsoft Windows On-Screen Keyboard Privilege Escalation Vulnerability (2975685)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-039

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow remote attackers to gain escalated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight
The flaw is triggered when executing the On-Screen keyboard from within the context of a low integrity process.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows On-Screen Keyboard Privilege Escalation Vulnerability (297568.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804472
Version used: `2023-07-27T05:05:08Z`

References
```
cve: CVE-2014-2781
url: https://support.microsoft.com/kb/2973201
url: http://www.securityfocus.com/bid/68397
url: https://support.microsoft.com/kb/2973906
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-039
cert-bund: CB-K14/0838
```

High (CVSS: 7.5)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4054518)

Summary
This host is missing a critical security update according to Microsoft KB4054518

Vulnerability Detection Result

```
Vulnerable range:  Less than 6.1.7601.23963
File checked:      C:\Windows\system32\Win32k.sys
File version:      6.1.7601.17514
```

Impact
Successful exploitation will allow an attacker who successfully exploited this vulnerability to execute code on the target system, gain the same user rights as the current user, obtain information to further compromise the user's system and could attempt a brute-force attack to disclose the password.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- An error in RPC if the server has Routing and Remote Access enabled.
- Internet Explorer improperly accesses objects in memory.
- Internet Explorer improperly handles objects in memory.
- Scripting engine handles objects in memory in Microsoft browsers.
- Windows its:// protocol handler unnecessarily sends traffic to a remote site in order to determine the zone of a provided URL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4054518)`
OID:1.3.6.1.4.1.25623.1.0.812245
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-11885
cve: CVE-2017-11886
cve: CVE-2017-11887
cve: CVE-2017-11890
cve: CVE-2017-11894
cve: CVE-2017-11895
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-11901
cve: CVE-2017-11903
cve: CVE-2017-11906
cve: CVE-2017-11907
cve: CVE-2017-11912
cve: CVE-2017-11913
cve: CVE-2017-11919
cve: CVE-2017-11927
cve: CVE-2017-11930
url: https://support.microsoft.com/en-us/help/4054518
url: http://www.securityfocus.com/bid/102055
url: http://www.securityfocus.com/bid/102062
url: http://www.securityfocus.com/bid/102063
url: http://www.securityfocus.com/bid/102082
url: http://www.securityfocus.com/bid/102053
url: http://www.securityfocus.com/bid/102054
url: http://www.securityfocus.com/bid/102046
url: http://www.securityfocus.com/bid/102047
url: http://www.securityfocus.com/bid/102078
url: http://www.securityfocus.com/bid/102045
url: http://www.securityfocus.com/bid/102092
url: http://www.securityfocus.com/bid/102091
url: http://www.securityfocus.com/bid/102093
url: http://www.securityfocus.com/bid/102095
url: http://www.securityfocus.com/bid/102058
cert-bund: CB-K17/2153
cert-bund: CB-K17/2152
cert-bund: CB-K17/2151
cert-bund: CB-K17/2149
dfn-cert: DFN-CERT-2017-2254
dfn-cert: DFN-CERT-2017-2253
dfn-cert: DFN-CERT-2017-2252
dfn-cert: DFN-CERT-2017-2248
```

High (CVSS: 7.5)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4088875)

Summary

This host is missing a critical security update according to Microsoft KB4088875

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24059
File checked:       C:\Windows\system32\win32k.sys
File version:       6.1.7601.17514
```

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow attacker to gain access to information, crash server and run arbitrary code in system mode.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Multiple flaws exist due to:
- When Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system.
- The way that the scripting engine handles objects in memory in Internet Explorer.
- When Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system.
- The Credential Security Support Provider protocol (CredSSP).
- Windows when the Microsoft Video Control mishandles objects in memory.
- When Windows Shell does not properly validate file copy destinations.
- When Internet Explorer fails a check, allowing sandbox escape.
- The Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass.
- The Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.
- When the Windows kernel improperly initializes objects in memory.
- When Windows Remote Assistance incorrectly processes XML External Entities (XXE).
- The way that the Windows Graphics Device Interface (GDI) handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4088875)`
OID:1.3.6.1.4.1.25623.1.0.812829
Version used: `2023-11-03T16:10:08Z`

References
```
cve: CVE-2018-0811
cve: CVE-2018-0813
cve: CVE-2018-0814
cve: CVE-2018-0815
cve: CVE-2018-0886
cve: CVE-2018-0888
cve: CVE-2018-0889
cve: CVE-2018-0891
cve: CVE-2018-0894
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2018-0895
cve: CVE-2018-0896
cve: CVE-2018-0897
cve: CVE-2018-0898
cve: CVE-2018-0899
cve: CVE-2018-0900
cve: CVE-2018-0901
cve: CVE-2018-0904
cve: CVE-2018-0927
cve: CVE-2018-0929
cve: CVE-2018-0932
cve: CVE-2018-0935
cve: CVE-2018-0942
cve: CVE-2018-0816
cve: CVE-2018-0817
cve: CVE-2018-0868
cve: CVE-2018-0878
cve: CVE-2018-0881
cve: CVE-2018-0883
cve: CVE-2018-0885
url: https://support.microsoft.com/en-us/help/4088875
url: http://www.securityfocus.com/bid/103232
url: http://www.securityfocus.com/bid/103250
url: http://www.securityfocus.com/bid/103251
url: http://www.securityfocus.com/bid/103234
url: http://www.securityfocus.com/bid/103265
url: http://www.securityfocus.com/bid/103262
url: http://www.securityfocus.com/bid/103295
url: http://www.securityfocus.com/bid/103309
url: http://www.securityfocus.com/bid/103231
url: http://www.securityfocus.com/bid/103238
url: http://www.securityfocus.com/bid/103240
url: http://www.securityfocus.com/bid/103241
url: http://www.securityfocus.com/bid/103242
url: http://www.securityfocus.com/bid/103243
url: http://www.securityfocus.com/bid/103244
url: http://www.securityfocus.com/bid/103245
url: http://www.securityfocus.com/bid/103246
url: http://www.securityfocus.com/bid/103310
url: http://www.securityfocus.com/bid/103299
url: http://www.securityfocus.com/bid/103307
url: http://www.securityfocus.com/bid/103298
url: http://www.securityfocus.com/bid/103312
url: http://www.securityfocus.com/bid/103248
url: http://www.securityfocus.com/bid/103249
url: http://www.securityfocus.com/bid/103236
url: http://www.securityfocus.com/bid/103230
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/103256
url: http://www.securityfocus.com/bid/103259
url: http://www.securityfocus.com/bid/103261
cert-bund: CB-K18/0461
cert-bund: CB-K18/0456
cert-bund: CB-K18/0455
cert-bund: CB-K18/0454
dfn-cert: DFN-CERT-2020-1810
dfn-cert: DFN-CERT-2019-0142
dfn-cert: DFN-CERT-2018-0494
dfn-cert: DFN-CERT-2018-0493
dfn-cert: DFN-CERT-2018-0491
dfn-cert: DFN-CERT-2018-0487
```

High (CVSS: 7.5)
NVT: Microsoft .NET Framework Information Disclosure Vulnerability (KB4480059)

Summary
This host is missing an important security update according to Microsoft KB4480059

Vulnerability Detection Result

```
Vulnerable range:  4.0.30319.30000 - 4.0.30319.36489
File checked:      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\system.dll
File version:      4.0.30319.34209
```

Impact
Successful exploitation will allow an attacker who successfully exploited the vulnerability to retrieve content, that is normally restricted, from a web application.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 4.5.2 on Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
The flaw exists due to an error which allows to bypass CORS configuration.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Information Disclosure Vulnerability (KB4480059)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.814720
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2019-0545
url: https://support.microsoft.com/en-us/help/4480059
url: http://www.securityfocus.com/bid/106405
cert-bund: CB-K19/0020
dfn-cert: DFN-CERT-2019-0052
dfn-cert: DFN-CERT-2019-0049
```

High (CVSS: 7.5)
NVT: Microsoft .NET Framework Information Disclosure Vulnerability (KB4344149)

Summary

This host is missing an important security update according to Microsoft KB4344149

Vulnerability Detection Result

```
Vulnerable range:   4.0.30319.30000 - 4.0.30319.36459
File checked:       C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\system.dll
File version:       4.0.30319.34209
```

Impact

Successful exploitation will allow an attacker to access information in multi-tenant environments.

Solution:

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

.NET Framework 4.5.2 for Windows 7 SP1, Server 2008 R2 SP1, and Server 2008 SP2

Vulnerability Insight

The flaw exists when .NET Framework is used in high-load/high-density network connections where content from one stream can blend into another stream.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Information Disclosure Vulnerability (KB4344149)`
OID:1.3.6.1.4.1.25623.1.0.813763
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2018-8360
url: https://support.microsoft.com/en-us/help/4344149
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0861
dfn-cert: DFN-CERT-2018-1604
```

High (CVSS: 7.5)
NVT: Microsoft .NET Framework Information Disclosure Vulnerability (3170048)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-091.

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\System.Data.d
↪ll
File version:     4.0.30319.34209
Vulnerable range: 4.0.30319.30000 - 4.0.30319.34296
```

Impact
Successful exploitation will allow remote attackers to gain access to potentially sensitive information.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6/4.6.1

Vulnerability Insight
Flaw exists as .NET Framework improperly parses XML input containing a reference to an external entity.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Information Disclosure Vulnerability (3170048)`
OID:1.3.6.1.4.1.25623.1.0.807856
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3255
url: https://support.microsoft.com/en-us/kb/3170048
url: https://support.microsoft.com/en-us/kb/3163912
url: https://support.microsoft.com/en-us/kb/3172985
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://technet.microsoft.com/library/security/MS16-091
cert-bund: CB-K16/1057
```

High (CVSS: 7.5)
NVT: Microsoft .NET Framework DoS Vulnerability (KB5012329)

Summary
This host is missing an important security update according to Microsoft KB5012329

Vulnerability Detection Result

```
Vulnerable range:   4.0.30319.30000 - 4.0.30319.36729
File checked:       C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\System.web.d
↪ll
File version:       4.0.30319.34209
```

Impact
Successful exploitation will allow an attacker to cause a denial of service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight
The flaw exists due to an input validation error in an unknown processing in .NET Framework.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework DoS Vulnerability (KB5012329)`
OID:1.3.6.1.4.1.25623.1.0.820062
Version used: `2022-04-28T03:04:10Z`

References

```
cve: CVE-2022-26832
url: https://support.microsoft.com/en-us/help/5012329
cert-bund: WID-SEC-2022-1251
cert-bund: CB-K22/0433
dfn-cert: DFN-CERT-2022-0812
```

High (CVSS: 7.5)
NVT: Microsoft .NET Framework DoS Vulnerability (KB5009719)

Summary
This host is missing an important security update according to Microsoft KB5009719

Vulnerability Detection Result

```
Vulnerable range:  4.0.30319.30000 - 4.0.30319.36719
File checked:      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.web.dl
↪l
File version:      4.0.30319.34209
```

Impact
Successful exploitation will allow an attacker to conduct a denial of service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight
The flaw exists due to an error in .NET Framework which allows an unauthenticated attacker to cause a denial of service on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework DoS Vulnerability (KB5009719)`
OID:1.3.6.1.4.1.25623.1.0.818943
Version used: `2022-01-24T03:04:40Z`

References

```
cve: CVE-2022-21911
url: https://support.microsoft.com/en-us/help/5009719
cert-bund: WID-SEC-2022-1251
cert-bund: CB-K22/0041
dfn-cert: DFN-CERT-2022-0048
```

High (CVSS: 7.5)
NVT: Oracle Java SE Security Update (jul2021) 02 - Windows

Summary
This host is missing a security update according to Oracle.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to have an impact on integrity, availability and confidentiality.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u291 (1.8.0.291) and earlier, 11.0.11 and earlier, 16.0.1 and earlier on Windows.

Vulnerability Insight

Multiple flaws are due to multiple errors in 'Libraries' and 'Networking' components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2021) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.818169

Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-2388
url: https://www.oracle.com/security-alerts/cpujul2021.html#AppendixJAVA
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-0464
cert-bund: CB-K21/0981
cert-bund: CB-K21/0783
dfn-cert: DFN-CERT-2022-0366
dfn-cert: DFN-CERT-2022-0074
```

High (CVSS: 7.5)
NVT: Oracle Java SE Security Update (jul2021) 02 - Windows

Summary

This host is missing a security update according to Oracle.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to have an impact on integrity, availability and confidentiality.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u291 (1.8.0.291) and earlier, 11.0.11 and earlier, 16.0.1 and earlier on Windows.

Vulnerability Insight

Multiple flaws are due to multiple errors in 'Libraries' and 'Networking' components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2021) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.818169

Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-2388
url: https://www.oracle.com/security-alerts/cpujul2021.html#AppendixJAVA
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-0464
cert-bund: CB-K21/0981
cert-bund: CB-K21/0783
dfn-cert: DFN-CERT-2022-0366
dfn-cert: DFN-CERT-2022-0074
```

High (CVSS: 7.5)

NVT: Oracle Java SE Security Update (apr2022) - Windows

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
```

. . . continues on next page . . .

... continued from previous page ...

path / port: C:\Program Files\Java\jre1.8.0_251

Impact

Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u321 (1.8.0.321) and earlier, 7u331 (1.7.0.331) and earlier, 11.x through 11.0.14, 17.x through 17.0.2, 18 on Windows.

Vulnerability Insight

Multiple flaws are due to unspecified errors in 'Libraries', 'JAXP' and 'JNDI' components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Oracle Java SE Security Update (apr2022) - Windows

OID:1.3.6.1.4.1.25623.1.0.820086

Version used: 2023-10-19T05:05:21Z

References

cve: CVE-2022-21449
cve: CVE-2022-21476
cve: CVE-2022-21426
cve: CVE-2022-21496
cve: CVE-2022-21434
cve: CVE-2022-21443
url: https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixJAVA
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-0840
cert-bund: WID-SEC-2022-1434
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1321
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1066
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0871
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0398
cert-bund: WID-SEC-2022-0300

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0287
cert-bund: WID-SEC-2022-0200
cert-bund: WID-SEC-2022-0028
cert-bund: CB-K22/0470
dfn-cert: DFN-CERT-2023-1425
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-1174
dfn-cert: DFN-CERT-2023-1139
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0819
dfn-cert: DFN-CERT-2022-1955
dfn-cert: DFN-CERT-2022-1704
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1323
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0871
```

High (CVSS: 7.5)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3124903)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS16-001.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: 8.0.7601.17000 - 8.0.7601.19103
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code and gain elevated privileges on the affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple flaws exist due to:
- An error due to improper handling of objects in memory,
- Improper enforcing of cross-domain policies.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Explorer Multiple Vulnerabilities (3124903)`
OID:1.3.6.1.4.1.25623.1.0.806659
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0002
cve: CVE-2016-0005
url: https://support.microsoft.com/en-us/kb/3124903
url: https://support.microsoft.com/en-us/kb/3124275
url: https://support.microsoft.com/en-us/kb/3124263
url: https://technet.microsoft.com/library/security/MS16-001
cert-bund: CB-K16/0052
```

High (CVSS: 7.5)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (KB4018271)

Summary
This host is missing a critical security update according to Microsoft security updates KB4018271.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Mshtml.dll
File version:     8.0.7601.17514
Vulnerable range: Less than 11.0.9600.18666
```

Impact
Successful exploitation will allow attacker to trick a user by redirecting the user to a specially crafted website, loading of unsecure content (HTTP) from secure locations (HTTPS) and to execute arbitrary code in the context of the current user.If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs, view, change, or delete data or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Internet Explorer version 9.x, 10.x and 11.x.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to:

- An error in the way JavaScript scripting engines handle objects in memory in Microsoft browsers.
- An error when Microsoft browsers render SmartScreen Filter.
- An error when Internet Explorer improperly accesses objects in memory.
- An unspecified error.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Internet Explorer Multiple Vulnerabilities (KB4018271)`

OID:1.3.6.1.4.1.25623.1.0.811032

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2017-0064
cve: CVE-2017-0222
cve: CVE-2017-0226
cve: CVE-2017-0228
cve: CVE-2017-0231
cve: CVE-2017-0238
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4018271
url: http://www.securityfocus.com/bid/98121
url: http://www.securityfocus.com/bid/98127
url: http://www.securityfocus.com/bid/98139
url: http://www.securityfocus.com/bid/98164
url: http://www.securityfocus.com/bid/98173
url: http://www.securityfocus.com/bid/98237
url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017
↪-0222
url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017
↪-0064
url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017
↪-0226
url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017
↪-0228
url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017
↪-0231
url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017
↪-0238
cert-bund: CB-K17/1378
cert-bund: CB-K17/0786
cert-bund: CB-K17/0781
dfn-cert: DFN-CERT-2017-1437
dfn-cert: DFN-CERT-2017-0810
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0809
```

High (CVSS: 7.5)
NVT: Apache Log4j 1.2.x RCE Vulnerability (Windows, Dec 2021) - Version Check

Summary
Apache Log4j is prone to a remote code execution (RCE) vulnerability in JMSAppender.

Vulnerability Detection Result

```
Installed version: 1.2.17
Fixed version:     None
Installation
path / port:       C:\Program Files\elasticsearch-1.1.1\lib\log4j-1.2.17.jar
```

Solution:
Solution type: WillNotFix
No solution was made available by the vendor.
Note: Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Affected Software/OS
Apache Log4j version 1.2.x.

Vulnerability Insight
JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228.
Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Log4j 1.2.x RCE Vulnerability (Windows, Dec 2021) - Version Check`
OID:1.3.6.1.4.1.25623.1.0.117843
Version used: `2022-01-10T03:03:27Z`

References

```
cve: CVE-2021-4104
url: https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0107
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1770
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-1189
cert-bund: WID-SEC-2022-1015
cert-bund: WID-SEC-2022-0927
cert-bund: WID-SEC-2022-0628
cert-bund: WID-SEC-2022-0520
cert-bund: CB-K22/0066
cert-bund: CB-K21/1291
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2022-1813
dfn-cert: DFN-CERT-2022-1472
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2022-0292
dfn-cert: DFN-CERT-2022-0204
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0015
```

High (CVSS: 7.5)
NVT: Apache Log4j 1.2.x RCE Vulnerability (Windows, Dec 2021) - Version Check

Summary
Apache Log4j is prone to a remote code execution (RCE) vulnerability in JMSAppender.

Vulnerability Detection Result

```
Installed version: 1.2.15
Fixed version:     None
Installation
path / port:       C:\Program Files\Apache Software Foundation\tomcat\apache-tom
↪cat-8.0.33\webapps\axis2\WEB-INF\lib\log4j-1.2.15.jar
```

Solution:
Solution type: WillNotFix
No solution was made available by the vendor.
Note: Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Affected Software/OS
Apache Log4j version 1.2.x.

Vulnerability Insight
JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228.

. . . continues on next page . . .

. . . continued from previous page . . .

Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Log4j 1.2.x RCE Vulnerability (Windows, Dec 2021) - Version Check`

OID:1.3.6.1.4.1.25623.1.0.117843

Version used: `2022-01-10T03:03:27Z`

References

```
cve: CVE-2021-4104
url: https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0107
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1770
cert-bund: WID-SEC-2022-1189
cert-bund: WID-SEC-2022-1015
cert-bund: WID-SEC-2022-0927
cert-bund: WID-SEC-2022-0628
cert-bund: WID-SEC-2022-0520
cert-bund: CB-K22/0066
cert-bund: CB-K21/1291
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2022-1813
dfn-cert: DFN-CERT-2022-1472
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2022-0292
dfn-cert: DFN-CERT-2022-0204
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0015
```

High (CVSS: 7.5)
NVT: Microsoft .NET Framework Authentication Bypass and Spoofing Vulnerabilities (2836440)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-040.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation could allow an attacker to bypass security mechanism and gain access to restricted endpoint functions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 2.0 Service Pack 2

Vulnerability Insight
The flaws are due to
- Improper validation of XML signatures by the CLR
- Error within the WCF endpoint authentication mechanism when handling queries

Vulnerability Detection Method
Details: `Microsoft .NET Framework Authentication Bypass and Spoofing Vulnerabilities (28.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903308
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2013-1336
cve: CVE-2013-1337
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-040
url: http://www.securityfocus.com/bid/59789
url: http://www.securityfocus.com/bid/59790
dfn-cert: DFN-CERT-2013-0895
```

High (CVSS: 7.5)
NVT: Microsoft .NET Framework Denial of Service Vulnerabilities (3137893)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-019.

Vulnerability Detection Result
```
File checked:     C:\Windows\Microsoft.NET\Framework64\v2.0.50727System.Xml.dll
File version:     2.0.50727.5420
Vulnerable range: Less than 2.0.50727.5495
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to gain access to sensitive information or disrupt the availability of applications that use the .NET framework.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6 and 4.6.1

Vulnerability Insight

Multiple flaws exist as,

- Application fails to properly handle certain Extensible Stylesheet Language Transformations (XSLT).
- The .NET's Windows Forms (WinForms) improperly handles icon data.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Denial of Service Vulnerabilities (3137893)`

OID:1.3.6.1.4.1.25623.1.0.806681

Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2016-0033
cve: CVE-2016-0047
url: https://support.microsoft.com/en-us/kb/3137893
url: https://technet.microsoft.com/library/security/MS16-019
cert-bund: CB-K16/0220
```

High (CVSS: 7.5)

NVT: Microsoft .NET Framework Denial of Service Vulnerabilities (3137893)

Summary

This host is missing an important security update according to Microsoft Bulletin MS16-019.

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v2.0.50727System.Drawing.
↪dll
File version:     2.0.50727.5420
Vulnerable range: Less than 2.0.50727.5495
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to gain access to sensitive information or disrupt the availability of applications that use the .NET framework.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6 and 4.6.1

Vulnerability Insight

Multiple flaws exist as,

- Application fails to properly handle certain Extensible Stylesheet Language Transformations (XSLT).
- The .NET's Windows Forms (WinForms) improperly handles icon data.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Denial of Service Vulnerabilities (3137893)`

OID:1.3.6.1.4.1.25623.1.0.806681

Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2016-0033
cve: CVE-2016-0047
url: https://support.microsoft.com/en-us/kb/3137893
url: https://technet.microsoft.com/library/security/MS16-019
cert-bund: CB-K16/0220
```

High (CVSS: 7.5)

NVT: Microsoft .NET Framework Multiple DoS Vulnerabilities (KB4499406)

Summary

This host is missing an important security update according to Microsoft KB4499406

Vulnerability Detection Result

```
Vulnerable range:   4.0.30319.30000 - 4.0.30319.36542
File checked:       C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.dll
File version:       4.0.30319.34209
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow an attacker to cause a denial of service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 on Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors when .NET Framework or .NET Core improperly handle web requests.
- An error when .NET Framework improperly handles objects in heap memory.
- An error when .NET Framework and .NET Core improperly process RegEx strings.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft .NET Framework Multiple DoS Vulnerabilities (KB4499406)`
OID:1.3.6.1.4.1.25623.1.0.815110
Version used: `2023-10-27T16:11:32Z`

References
```
cve: CVE-2019-0864
cve: CVE-2019-0820
cve: CVE-2019-0980
cve: CVE-2019-0981
url: https://support.microsoft.com/en-us/help/4499406
url: http://www.securityfocus.com/bid/108241
url: http://www.securityfocus.com/bid/108245
url: http://www.securityfocus.com/bid/108232
url: http://www.securityfocus.com/bid/108207
url: https://support.microsoft.com/en-us/help/4495606
url: https://support.microsoft.com/en-us/help/4495596
url: https://support.microsoft.com/en-us/help/4495588
url: https://support.microsoft.com/en-us/help/4495626
cert-bund: CB-K19/0419
dfn-cert: DFN-CERT-2019-1049
dfn-cert: DFN-CERT-2019-1048
dfn-cert: DFN-CERT-2019-1007
dfn-cert: DFN-CERT-2019-0962
```

High (CVSS: 7.5)
NVT: Oracle Java SE Security Update (jul2022) - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_211
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jdk1.8.0_211
```

Impact
Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 7u343 (1.7.0.343) and earlier, 8u333 (1.8.0.333) and earlier, 11.x through 11.0.15.1, 17.x through 17.0.3.1, 18.x through 18.0.1.1 on Windows.

Vulnerability Insight
Multiple flaws are due to unspecified errors in 'Libraries', 'JAXP' and 'Hotspot' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jul2022) - Windows`
OID:1.3.6.1.4.1.25623.1.0.821189
Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-34169
cve: CVE-2022-21541
cve: CVE-2022-21540
cve: CVE-2022-21549
url: https://www.oracle.com/security-alerts/cpujul2022.html#AppendixJAVA
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0890
cert-bund: WID-SEC-2024-0870
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0788
cert-bund: WID-SEC-2024-0671
cert-bund: WID-SEC-2024-0124
cert-bund: WID-SEC-2023-2368
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1032
cert-bund: WID-SEC-2023-1017
cert-bund: WID-SEC-2023-0553
cert-bund: WID-SEC-2023-0122
cert-bund: WID-SEC-2022-1244
cert-bund: WID-SEC-2022-0759
cert-bund: WID-SEC-2022-0746
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2023-0899
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2321
dfn-cert: DFN-CERT-2022-1955
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1607
dfn-cert: DFN-CERT-2022-1606
```

High (CVSS: 7.5)
NVT: Oracle Java SE Security Update (jul2022) - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 7u343 (1.7.0.343) and earlier, 8u333 (1.8.0.333) and earlier, 11.x through 11.0.15.1, 17.x through 17.0.3.1, 18.x through 18.0.1.1 on Windows.

Vulnerability Insight
Multiple flaws are due to unspecified errors in 'Libraries', 'JAXP' and 'Hotspot' components.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2022) - Windows`

OID:1.3.6.1.4.1.25623.1.0.821189

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-34169
cve: CVE-2022-21541
cve: CVE-2022-21540
cve: CVE-2022-21549
url: https://www.oracle.com/security-alerts/cpujul2022.html#AppendixJAVA
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0890
cert-bund: WID-SEC-2024-0870
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0788
cert-bund: WID-SEC-2024-0671
cert-bund: WID-SEC-2024-0124
cert-bund: WID-SEC-2023-2368
cert-bund: WID-SEC-2023-1032
cert-bund: WID-SEC-2023-1017
cert-bund: WID-SEC-2023-0553
cert-bund: WID-SEC-2023-0122
cert-bund: WID-SEC-2022-1244
cert-bund: WID-SEC-2022-0759
cert-bund: WID-SEC-2022-0746
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2023-0899
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2321
dfn-cert: DFN-CERT-2022-1955
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1607
dfn-cert: DFN-CERT-2022-1606
```

High (CVSS: 7.5)
NVT: Oracle Java SE Security Update (jul2022) - Windows

Summary

Oracle Java SE is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 7u343 (1.7.0.343) and earlier, 8u333 (1.8.0.333) and earlier, 11.x through 11.0.15.1, 17.x through 17.0.3.1, 18.x through 18.0.1.1 on Windows.

Vulnerability Insight

Multiple flaws are due to unspecified errors in 'Libraries', 'JAXP' and 'Hotspot' components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2022) - Windows`

OID:1.3.6.1.4.1.25623.1.0.821189

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-34169
cve: CVE-2022-21541
cve: CVE-2022-21540
cve: CVE-2022-21549
url: https://www.oracle.com/security-alerts/cpujul2022.html#AppendixJAVA
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0890
cert-bund: WID-SEC-2024-0870
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0788
cert-bund: WID-SEC-2024-0671
cert-bund: WID-SEC-2024-0124
cert-bund: WID-SEC-2023-2368
cert-bund: WID-SEC-2023-1032
cert-bund: WID-SEC-2023-1017
cert-bund: WID-SEC-2023-0553
cert-bund: WID-SEC-2023-0122
cert-bund: WID-SEC-2022-1244
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0759
cert-bund: WID-SEC-2022-0746
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2023-0899
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2321
dfn-cert: DFN-CERT-2022-1955
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1607
dfn-cert: DFN-CERT-2022-1606
```

High (CVSS: 7.5)
NVT: Apache Log4j 1.2.x RCE Vulnerability (Windows, Dec 2021) - Version Check

Summary
Apache Log4j is prone to a remote code execution (RCE) vulnerability in JMSAppender.

Vulnerability Detection Result

```
Installed version: 1.2.15
Fixed version:     None
Installation
path / port:       C:\ManageEngine\DesktopCentral_Server\lib\log4j-1.2.15.jar
```

Solution:
Solution type: WillNotFix
No solution was made available by the vendor.
Note: Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Affected Software/OS
Apache Log4j version 1.2.x.

Vulnerability Insight
JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228.
Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Apache Log4j 1.2.x RCE Vulnerability (Windows, Dec 2021) - Version Check
OID:1.3.6.1.4.1.25623.1.0.117843
Version used: 2022-01-10T03:03:27Z

References

```
cve: CVE-2021-4104
url: https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0107
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1770
cert-bund: WID-SEC-2022-1189
cert-bund: WID-SEC-2022-1015
cert-bund: WID-SEC-2022-0927
cert-bund: WID-SEC-2022-0628
cert-bund: WID-SEC-2022-0520
cert-bund: CB-K22/0066
cert-bund: CB-K21/1291
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2022-1813
dfn-cert: DFN-CERT-2022-1472
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2022-0292
dfn-cert: DFN-CERT-2022-0204
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0015
```

High (CVSS: 7.5)
NVT: Apache Log4j 1.2.x RCE Vulnerability (Windows, Dec 2021) - Version Check

Summary

Apache Log4j is prone to a remote code execution (RCE) vulnerability in JMSAppender.

Vulnerability Detection Result

```
Installed version: 1.2.17
Fixed version:     None
Installation
path / port:       C:\Program Files\Apache Software Foundation\tomcat\apache-tom
↪cat-8.0.33\webapps\struts2-rest-showcase\WEB-INF\lib\log4j-1.2.17.jar
```

Solution:

Solution type: WillNotFix

No solution was made available by the vendor.

. . . continues on next page . . .

. . . continued from previous page . . .

Note: Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Affected Software/OS
Apache Log4j version 1.2.x.

Vulnerability Insight
JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228.
Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Log4j 1.2.x RCE Vulnerability (Windows, Dec 2021) - Version Check`
OID:1.3.6.1.4.1.25623.1.0.117843
Version used: `2022-01-10T03:03:27Z`

References
```
cve: CVE-2021-4104
url: https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0107
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1770
cert-bund: WID-SEC-2022-1189
cert-bund: WID-SEC-2022-1015
cert-bund: WID-SEC-2022-0927
cert-bund: WID-SEC-2022-0628
cert-bund: WID-SEC-2022-0520
cert-bund: CB-K22/0066
cert-bund: CB-K21/1291
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2022-1813
dfn-cert: DFN-CERT-2022-1472
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0325
dfn-cert: DFN-CERT-2022-0292
dfn-cert: DFN-CERT-2022-0204
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0015
```

High (CVSS: 7.5)
NVT: Microsoft Windows RPC Security Feature Bypass Vulnerability (2978668)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-047

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to bypass the ASLR security feature in conjunction with another vulnerability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
The flaw is due to RPC improperly frees messages that the server rejects as malformed, allowing an attacker to fill up the address space of a process.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows RPC Security Feature Bypass Vulnerability (2978668)`
OID:1.3.6.1.4.1.25623.1.0.802078
Version used: `2023-07-26T05:05:09Z`

References
```
cve: CVE-2014-0316
url: https://support.microsoft.com/kb/2978668
url: http://www.securityfocus.com/bid/69097
url: https://technet.microsoft.com/library/security/MS14-047
cert-bund: CB-K14/1013
```

High (CVSS: 7.5)
NVT: Microsoft .NET Framework Security Bypass Vulnerability (4019112)

Summary
This host is missing an important security update according to Microsoft KB4019112

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\system.dll
File version:     4.0.30319.34209
Vulnerable range: 4.0.30319.30000 - 4.0.30319.36391
```

Impact

Successful exploitation will allow remote attackers to bypass certain security restrictions and perform unauthorized actions.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6/4.6.1
- Microsoft .NET Framework 4.6.2

Vulnerability Insight

Flaw exists when Microsoft .NET Framework (and .NET Core) components do not completely validate certificates.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Security Bypass Vulnerability (4019112)`

OID:1.3.6.1.4.1.25623.1.0.811039

Version used: `2024-03-05T05:05:54Z`

References

```
cve: CVE-2017-0248
url: https://support.microsoft.com/en-us/help/4019112
url: http://www.securityfocus.com/bid/98117
cert-bund: CB-K17/0788
dfn-cert: DFN-CERT-2017-0815
```

High (CVSS: 7.5)

NVT: Microsoft .NET Framework Security Bypass Vulnerability (4019115)

Summary

This host is missing an important security update according to Microsoft KB4019115

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\system.manage
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ment.dll
File version:     4.0.30319.34209
Vulnerable range: 4.0.30319.30000 - 4.0.30319.36391
```

Impact

Successful exploitation will allow remote attackers to bypass certain security restrictions and perform unauthorized actions.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 4.5.2
- Microsoft .NET Framework 4.6

Vulnerability Insight

Flaw exists when Microsoft .NET Framework (and .NET Core) components do not completely validate certificates.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Security Bypass Vulnerability (4019115)`

OID:1.3.6.1.4.1.25623.1.0.811036

Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0248
url: https://support.microsoft.com/en-us/help/4019115
url: http://www.securityfocus.com/bid/98117
url: https://support.microsoft.com/en-us/help/4019115
cert-bund: CB-K17/0788
dfn-cert: DFN-CERT-2017-0815
```

High (CVSS: 7.5)

NVT: Microsoft .NET Framework Security Feature Bypass And DoS Vulnerabilities (KB4054995)

Summary

This host is missing a critical security update according to Microsoft Security Updates KB4054995.

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\system.runtim
↪e.remoting.dll
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
File version:     4.0.30319.34209
Vulnerable range: 4.0.30319.30000 - 4.0.30319.36414
```

Impact

Successful exploitation will allow an attacker who successfully exploited this vulnerability to cause a denial of service against a .NET application and also to bypass security.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 4.5.2.

Vulnerability Insight

Multiple flaws exist due to:

- .NET, and .NET core, improperly process XML documents.
- Microsoft .NET Framework (and .NET Core) components do not completely validate certificates.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Security Feature Bypass And DoS Vulnerabilities (KB405.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.812709

Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-0764
cve: CVE-2018-0786
url: https://support.microsoft.com/en-us/help/4054995
cert-bund: CB-K18/0375
cert-bund: CB-K18/0053
dfn-cert: DFN-CERT-2018-0405
dfn-cert: DFN-CERT-2018-0061
```

High (CVSS: 7.5)

NVT: Microsoft VBScript Scripting Engine OLE Automation Memory Corruption Vulnerability (3188724)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS16-116

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Oleaut32.dll
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23512
```

Impact

Successful exploitation will allow remote attacker to execute arbitrary code in the context of the current user.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight

The flaw is due to an improper way of accessing objects in the memory by Microsoft OLE Automation mechanism and the VBScript Scripting Engine in Internet Explorer.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft VBScript Scripting Engine OLE Automation Memory Corruption Vulnerabil.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.809040

Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-3375
url: https://support.microsoft.com/en-us/kb/3188724
url: http://www.securityfocus.com/bid/92835
url: https://technet.microsoft.com/en-us/library/security/ms16-116
cert-bund: CB-K16/1406
cert-bund: CB-K16/1403
```

High (CVSS: 7.5)

NVT: Oracle Java SE Security Update (apr2022) - Windows

Summary

Oracle Java SE is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u321 (1.8.0.321) and earlier, 7u331 (1.7.0.331) and earlier, 11.x through 11.0.14, 17.x through 17.0.2, 18 on Windows.

Vulnerability Insight

Multiple flaws are due to unspecified errors in 'Libraries', 'JAXP' and 'JNDI' components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (apr2022) - Windows`

OID:1.3.6.1.4.1.25623.1.0.820086

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-21449
cve: CVE-2022-21476
cve: CVE-2022-21426
cve: CVE-2022-21496
cve: CVE-2022-21434
cve: CVE-2022-21443
url: https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixJAVA
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-0840
cert-bund: WID-SEC-2022-1434
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1321
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1066
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0871
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0398
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0287
cert-bund: WID-SEC-2022-0200
cert-bund: WID-SEC-2022-0028
cert-bund: CB-K22/0470
dfn-cert: DFN-CERT-2023-1425
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-1174
dfn-cert: DFN-CERT-2023-1139
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0819
dfn-cert: DFN-CERT-2022-1955
dfn-cert: DFN-CERT-2022-1704
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1323
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0871
```

High (CVSS: 7.5)
NVT: Microsoft Windows LSASS Local Denial of Service Vulnerability (3216771)

Summary

This host is missing an important security update according to Microsoft Bulletin MS17-004.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Lsass.exe
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.23642
```

Impact

Successful exploitation will allow attackers to cause a denial of service on the target system's LSASS service, which triggers an automatic reboot of the system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

... continued from previous page ...

Affected Software/OS

- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight

The flaw exists in the way the Local Security Authority Subsystem Service (LSASS) handles authentication requests.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows LSASS Local Denial of Service Vulnerability (3216771)`
OID:1.3.6.1.4.1.25623.1.0.809861
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0004
url: https://support.microsoft.com/en-us/kb/3216771
url: http://www.securityfocus.com/bid/95318
url: https://technet.microsoft.com/en-us/library/security/MS16-004
url: https://technet.microsoft.com/library/security/MS17-004
cert-bund: CB-K17/0038
dfn-cert: DFN-CERT-2017-0040
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Update (jan2024) 02 - Windows

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to compromise Oracle Java SE, which can result in unauthorized update, insert or delete access to critical data or all Oracle Java SE

Solution:

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS
Oracle Java SE version 8u391 and earlier 11.0.21, 17.0.9, 21.0.1 and earlier on Windows.

Vulnerability Insight
Multiple flaws exist due to multiple errors in the multiple components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2024) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832788
Version used: `2024-01-24T05:06:24Z`

References

```
cve: CVE-2024-20918
cve: CVE-2024-20952
cve: CVE-2024-20919
cve: CVE-2024-20921
cve: CVE-2024-20945
url: https://www.oracle.com/security-alerts/cpujan2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0121
dfn-cert: DFN-CERT-2024-0533
dfn-cert: DFN-CERT-2024-0502
dfn-cert: DFN-CERT-2024-0501
dfn-cert: DFN-CERT-2024-0500
dfn-cert: DFN-CERT-2024-0494
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0422
dfn-cert: DFN-CERT-2024-0417
dfn-cert: DFN-CERT-2024-0361
dfn-cert: DFN-CERT-2024-0354
dfn-cert: DFN-CERT-2024-0129
dfn-cert: DFN-CERT-2024-0128
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Update (apr2023) 01 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u361 and earlier, 11.0.18, 17.0.6, 20.0.0 and earlier on Windows.

Vulnerability Insight

Multiple flaws exist due to multiple errors in the networking components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (apr2023) 01 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832045

Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-21930
cve: CVE-2023-21937
cve: CVE-2023-21938
cve: CVE-2023-21939
cve: CVE-2023-21967
cve: CVE-2023-21968
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2112
cert-bund: WID-SEC-2023-1846
cert-bund: WID-SEC-2023-1011
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2493
dfn-cert: DFN-CERT-2023-2249
dfn-cert: DFN-CERT-2023-2240
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1879
dfn-cert: DFN-CERT-2023-1605
dfn-cert: DFN-CERT-2023-1418
dfn-cert: DFN-CERT-2023-1336
dfn-cert: DFN-CERT-2023-1304
dfn-cert: DFN-CERT-2023-0897
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0896
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Update (apr2023) 01 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u361 and earlier, 11.0.18, 17.0.6, 20.0.0 and earlier on Windows.

Vulnerability Insight
Multiple flaws exist due to multiple errors in the networking components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (apr2023) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832045
Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-21930
cve: CVE-2023-21937
cve: CVE-2023-21938
cve: CVE-2023-21939
cve: CVE-2023-21967
cve: CVE-2023-21968
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2112
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1846
cert-bund: WID-SEC-2023-1011
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2493
dfn-cert: DFN-CERT-2023-2249
dfn-cert: DFN-CERT-2023-2240
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1879
dfn-cert: DFN-CERT-2023-1605
dfn-cert: DFN-CERT-2023-1418
dfn-cert: DFN-CERT-2023-1336
dfn-cert: DFN-CERT-2023-1304
dfn-cert: DFN-CERT-2023-0897
dfn-cert: DFN-CERT-2023-0896
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Update (jan2024) 02 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to compromise Oracle Java SE, which can result in unauthorized update, insert or delete access to critical data or all Oracle Java SE

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u391 and earlier 11.0.21, 17.0.9, 21.0.1 and earlier on Windows.

Vulnerability Insight
Multiple flaws exist due to multiple errors in the multiple components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2024) 02 - Windows`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.832788
Version used: `2024-01-24T05:06:24Z`

References

```
cve: CVE-2024-20918
cve: CVE-2024-20952
cve: CVE-2024-20919
cve: CVE-2024-20921
cve: CVE-2024-20945
url: https://www.oracle.com/security-alerts/cpujan2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0121
dfn-cert: DFN-CERT-2024-0533
dfn-cert: DFN-CERT-2024-0502
dfn-cert: DFN-CERT-2024-0501
dfn-cert: DFN-CERT-2024-0500
dfn-cert: DFN-CERT-2024-0494
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0422
dfn-cert: DFN-CERT-2024-0417
dfn-cert: DFN-CERT-2024-0361
dfn-cert: DFN-CERT-2024-0354
dfn-cert: DFN-CERT-2024-0129
dfn-cert: DFN-CERT-2024-0128
```

High (CVSS: 7.2)
NVT: Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2709162)

Summary
This host is missing an important security update according to Microsoft Bulletin MS12-041.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to execute arbitrary code with kernel-mode privileges

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior

. . . continues on next page . . .

... continued from previous page ...

- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

Multiple flaws are due to:

- An error in win32k.sys within the string atom class name and lipboard format atom name handling and can be exploited to execute arbitrary code.
- An integer overflow error when handling the reference counter for font resources when loading TrueType fonts.
- A race condition error in win32k.sys when handling particular thread creation attempts and can be exploited to execute arbitrary code.

Vulnerability Detection Method

Details: `Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2709162)`

OID:1.3.6.1.4.1.25623.1.0.902917

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-1864
cve: CVE-2012-1865
cve: CVE-2012-1866
cve: CVE-2012-1867
cve: CVE-2012-1868
url: http://support.microsoft.com/kb/2709162
url: http://www.securityfocus.com/bid/53815
url: http://www.securityfocus.com/bid/53816
url: http://www.securityfocus.com/bid/53817
url: http://www.securityfocus.com/bid/53819
url: http://www.securityfocus.com/bid/53820
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-041
dfn-cert: DFN-CERT-2012-1124
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Driver Privilege Elevation Vulnerabilities (3034344)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-023.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to bypass security and gain restricted privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Multiple flaws exist:
- In the Windows kernel-mode driver that could allow the disclosure of kernel memory contents to an attacker.
- In the Windows kernel-mode driver that is caused when the kernel-mode driver fails to properly validate the calling threads token.
- In the Windows kernel-mode driver that could allow the disclosure of kernel memory contents to an attacker.
- In the Windows kernel-mode driver that could allow the disclosure of kernel memory contents to an attacker. This vulnerability is caused when the Windows kernel-mode driver dereferences a NULL pointer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel-Mode Driver Privilege Elevation Vulnerabilities (30343.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.805351
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-0077
cve: CVE-2015-0078
cve: CVE-2015-0094
cve: CVE-2015-0095
url: https://support.microsoft.com/kb/3034344
url: https://technet.microsoft.com/library/security/MS15-023
cert-bund: CB-K15/0319
dfn-cert: DFN-CERT-2015-0324
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Driver Privilege Elevation Vulnerabilities (3057839)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-061.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow remote attackers to bypass security, gain elevated privileges and execute arbitrary code on affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Multiple flaws exist due to:
- Improper handling of buffer elements by windows kernel-mode driver under certain conditions.
- Improper freeing of an object in memory by windows kernel-mode driver.
- Insufficient validation of certain data passed from user mode by the windows kernel-mode driver.
- Windows kernel-mode driver when it accesses an object in memory that has either not been correctly initialized or deleted.
- Windows kernel-mode driver when it improperly validates user input.
- Windows kernel-mode driver 'Win32k.sys' fails to properly free memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel-Mode Driver Privilege Elevation Vulnerabilities (30578.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.805582
Version used: `2023-07-25T05:05:58Z`

References
`cve: CVE-2015-1719`
`cve: CVE-2015-1720`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-1721
cve: CVE-2015-1722
cve: CVE-2015-1723
cve: CVE-2015-1724
cve: CVE-2015-1725
cve: CVE-2015-1726
cve: CVE-2015-1727
cve: CVE-2015-1768
cve: CVE-2015-2360
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3057839
url: http://www.securityfocus.com/bid/74999
url: http://www.securityfocus.com/bid/75000
url: http://www.securityfocus.com/bid/74998
url: http://www.securityfocus.com/bid/75005
url: http://www.securityfocus.com/bid/75009
url: http://www.securityfocus.com/bid/75010
url: http://www.securityfocus.com/bid/75006
url: http://www.securityfocus.com/bid/75012
url: http://www.securityfocus.com/bid/75008
url: http://www.securityfocus.com/bid/75024
url: http://www.securityfocus.com/bid/75025
url: https://technet.microsoft.com/en-us/library/security/ms15-061.aspx
cert-bund: CB-K15/0783
dfn-cert: DFN-CERT-2015-0827
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Driver Privilege Elevation Vulnerabilities (3070102)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-073.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to bypass security, gain elevated privileges and execute arbitrary code on affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight

Multiple flaws exist due to:

- An improper handling of buffer elements by windows kernel-mode driver under certain conditions.
- An improper freeing of an object in memory by windows kernel-mode driver.
- Improper handling of buffer elements by windows kernel-mode driver under certain conditions.
- Improper freeing of an object in memory by windows kernel-mode driver.
- Insufficient validation of certain data passed from user mode by the windows kernel-mode driver.
- Windows kernel-mode driver when it accesses an object in memory that has either not been correctly initialized or deleted.
- Windows kernel-mode driver when it improperly validates user input.
- Windows kernel-mode driver 'Win32k.sys' fails to properly free memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel-Mode Driver Privilege Elevation Vulnerabilities (30701.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.805074

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2363
cve: CVE-2015-2365
cve: CVE-2015-2366
cve: CVE-2015-2367
cve: CVE-2015-2381
cve: CVE-2015-2382
url: https://support.microsoft.com/en-us/kb/3070102
url: https://technet.microsoft.com/en-us/library/security/MS15-073
url: https://technet.microsoft.com/en-us/library/security/ms15-073
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1060
```

High (CVSS: 7.2)
NVT: Microsoft Windows Installer Service Privilege Escalation Vulnerability (2962490)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing an important security update according to Microsoft Bulletin MS14-049

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to gain escalated privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2

Vulnerability Insight

Flaw exists due to an error within the Windows Installer Service when handling a repair of a previously installed application

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Installer Service Privilege Escalation Vulnerability (2962490)`

OID:1.3.6.1.4.1.25623.1.0.804808

Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-1814
url: https://support.microsoft.com/kb/2918614
url: http://www.securityfocus.com/bid/69112
url: https://technet.microsoft.com/library/security/MS14-049
cert-bund: CB-K14/1013
```

High (CVSS: 7.2)

NVT: Microsoft Windows Kernel-Mode Driver RCE Vulnerabilities (3036220)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-010.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to bypass security and gain restricted privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight

The flaw is due to an error within the WebDAV kernel-mode driver (mrxdav.sys).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel-Mode Driver RCE Vulnerabilities (3036220)`

OID:1.3.6.1.4.1.25623.1.0.805337

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0003
cve: CVE-2015-0010
cve: CVE-2015-0057
cve: CVE-2015-0058
cve: CVE-2015-0059
cve: CVE-2015-0060
url: https://support.microsoft.com/kb/3013455
url: http://www.securityfocus.com/bid/72457
url: http://www.securityfocus.com/bid/72461
url: http://www.securityfocus.com/bid/72466
url: http://www.securityfocus.com/bid/72468
url: http://www.securityfocus.com/bid/72470
url: http://www.securityfocus.com/bid/72472
url: https://support.microsoft.com/kb/3023562
url: https://technet.microsoft.com/library/security/MS15-010
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K15/0171
dfn-cert: DFN-CERT-2015-0175
```

High (CVSS: 7.2)
NVT: Microsoft Windows Privilege Elevation Vulnerabilities (3049576)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-038.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow local users to gain privileges via a crafted application.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Flaws are due to:
- A type confusion flaw related to NtCreateTransactionManager that may result in the operating system failing to properly validate and enforce impersonation levels.
- The operating system failing to properly validate and enforce impersonation levels when handling an MS-DOS device name. This may allow a local attacker to gain elevated privileges.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Privilege Elevation Vulnerabilities (3049576)`
OID:1.3.6.1.4.1.25623.1.0.805065
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1643
cve: CVE-2015-1644
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://support.microsoft.com/kb/3045685
url: https://support.microsoft.com/kb/3045999
url: https://technet.microsoft.com/library/security/MS15-038
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2718523)

Summary
This host has important security update missing according to Microsoft Bulletin MS12-047.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to execute arbitrary code with kernel-mode privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Windows kernel-mode driver improperly validates parameters (when creating a hook procedure) and specific keyboard layouts, which can be exploited to execute arbitrary code.

Vulnerability Detection Method
Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2718.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903033
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-1890
cve: CVE-2012-1893
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://support.microsoft.com/kb/2718523
url: http://www.securityfocus.com/bid/54285
url: http://www.securityfocus.com/bid/54302
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-047
dfn-cert: DFN-CERT-2012-1330
```

High (CVSS: 7.2)
NVT: Microsoft Windows Winsock Elevation of Privilege Vulnerability (3104521)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-119.

Vulnerability Detection Result

```
File checked:     C:\Windowssystem32\Drivers\afd.sys
File version:     6.1.7601.17514
Vulnerable range: less than 6.1.7601.19031
```

Impact
Successful exploitation will allow attackers to gain elevated privileges of an affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Edge on Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Flaw is due to a double-free error in the Ancillary Function Driver within 'afd.sys'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Winsock Elevation of Privilege Vulnerability (3104521)`
OID:1.3.6.1.4.1.25623.1.0.805774
Version used: `2023-07-25T05:05:58Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2015-2478
url: https://support.microsoft.com/kb/3092601
url: https://technet.microsoft.com/library/security/ms15-119
cert-bund: CB-K15/1649
dfn-cert: DFN-CERT-2015-1742
```

High (CVSS: 7.2)
NVT: Microsoft Windows User Profile Service Privilege Escalation (3021674)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-003.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow local attacker to perform certain actions with higher privileges and potentially gain elevated privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2

Vulnerability Insight

Flaw is due to some weaknesses when creating directories and mounting user hives during the login process.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows User Profile Service Privilege Escalation (3021674)`

OID:1.3.6.1.4.1.25623.1.0.805126

Version used: `2023-07-25T05:05:58Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2015-0004
url: https://support.microsoft.com/kb/3021674
url: http://www.securityfocus.com/bid/71967
url: https://technet.microsoft.com/library/security/MS15-003
cert-bund: CB-K15/0038
dfn-cert: DFN-CERT-2015-0036
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2807986)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-027.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow remote attackers to compromise the affected system and possibly execute arbitrary code with System-level privileges.

Solution:

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

Multiple flaws are due to improper handling of objects in memory by the kernel-mode driver, which can be exploited by inserting a malicious USB device into the system.

Vulnerability Detection Method

Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2807.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903200
Version used: `2022-05-25T07:40:23Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-1285
cve: CVE-2013-1286
cve: CVE-2013-1287
url: http://support.microsoft.com/kb/2807986
url: http://www.securityfocus.com/bid/58359
url: http://www.securityfocus.com/bid/58360
url: http://www.securityfocus.com/bid/58361
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-027
dfn-cert: DFN-CERT-2013-0535
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2840221)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-046.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to gain escalated privileges or cause buffer overflow and execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to:
- A race condition error within the DirectX graphics kernel subsystem.
- An unspecified error within the Windows kernel-mode driver (win32k.sys)

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2840.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903208
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-1332
cve: CVE-2013-1333
cve: CVE-2013-1334
url: http://support.microsoft.com/kb/2829361
url: http://www.securityfocus.com/bid/59749
url: http://www.securityfocus.com/bid/59750
url: http://www.securityfocus.com/bid/59782
url: http://support.microsoft.com/kb/2830290
url: http://www.securelist.com/en/advisories/53385
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-046
dfn-cert: DFN-CERT-2013-0891
```

High (CVSS: 7.2)
NVT: Microsoft Windows TCP/IP Privilege Elevation Vulnerabilities (2688338)

Summary

This host is missing an important security update according to Microsoft Bulletin MS12-032.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow attackers to bypass certain security restrictions and gain escalated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 Service Pack 1
- Microsoft Windows Vista Service Pack 2 and prior
- Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight

The flaws are due to the way,
- Windows Firewall handles outbound broadcast packets.
- Windows TCP/IP stack handles the binding of an IPv6 address to a local interface.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Microsoft Windows TCP/IP Privilege Elevation Vulnerabilities (2688338)`
OID:1.3.6.1.4.1.25623.1.0.902676
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-0174
cve: CVE-2012-0179
url: http://support.microsoft.com/kb/2688338
url: http://www.securityfocus.com/bid/53349
url: http://www.securityfocus.com/bid/53352
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-032
dfn-cert: DFN-CERT-2012-0898
```

High (CVSS: 7.2)
NVT: Microsoft Windows PGM UAF Elevation of Privilege Vulnerability (3116130)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-133

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Rmcast.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19055
```

Impact

Successful exploitation will allow an authenticated user to execute code with elevated privileges that would allow them to install programs.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Edge on Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The flaw is due to some unspecified weakness in the Windows Pragmatic General Multicast (PGM) protocol.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows PGM UAF Elevation of Privilege Vulnerability (3116130)`

OID:1.3.6.1.4.1.25623.1.0.806775

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-6126
url: https://support.microsoft.com/en-us/kb/3116130
url: http://www.securityfocus.com/bid/78509
url: https://support.microsoft.com/en-us/kb/3109103
url: https://technet.microsoft.com/library/security/MS15-133
cert-bund: CB-K15/1804
dfn-cert: DFN-CERT-2015-1903
```

High (CVSS: 7.2)

NVT: Microsoft Windows Mount Manager Privilege Elevation Vulnerability (3082487)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-085.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow a local attacker to elevate privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

The flaw is due to improper symbolic link processing by the Mount Manager component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Mount Manager Privilege Elevation Vulnerability (3082487)`

OID:1.3.6.1.4.1.25623.1.0.806011

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1769
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3071756
url: http://www.securityfocus.com/bid/76222
url: https://technet.microsoft.com/library/security/MS15-085
cert-bund: CB-K15/1174
dfn-cert: DFN-CERT-2015-1236
```

High (CVSS: 7.2)

NVT: Microsoft Windows Graphics Component Privilege Elevation Vulnerability (3069392)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-072.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to gain elevated privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2
- Microsoft Windows Vista x32/x64 Edition Service Pack 2

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight

Flaw exists due to error when windows graphics component fails to properly process bitmap conversions.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Graphics Component Privilege Elevation Vulnerability (3069392)`

OID:1.3.6.1.4.1.25623.1.0.805920

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2364
url: https://support.microsoft.com/en-us/kb/3069392
url: https://technet.microsoft.com/en-us/library/security/MS15-072
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1060
```

High (CVSS: 7.2)

NVT: Microsoft Windows Remote Code Execution Vulnerability (3116162)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-132.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Catsrvut.dll
File version:     2001.12.8530.16385
Vulnerable range: Less than 2001.12.8531.19062
```

Impact

Successful exploitation will allow an attacker to take complete control of an affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight

Flaw exists due to an error in the windows which improperly validates input before loading libraries.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Remote Code Execution Vulnerability (3116162)`
OID:1.3.6.1.4.1.25623.1.0.806645
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-6128
cve: CVE-2015-6132
cve: CVE-2015-6133
url: https://support.microsoft.com/en-us/kb/3108371
url: http://www.securityfocus.com/bid/78612
url: http://www.securityfocus.com/bid/78614
url: http://www.securityfocus.com/bid/78615
url: https://support.microsoft.com/en-us/kb/3108347
url: https://support.microsoft.com/en-us/kb/3108381
url: https://support.microsoft.com/en-us/kb/3108371
url: https://technet.microsoft.com/library/security/MS15-132
cert-bund: CB-K15/1804
dfn-cert: DFN-CERT-2015-1903
```

High (CVSS: 7.2)
NVT: Microsoft Windows NDIS Elevation of Privilege Vulnerability (3101722)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-117.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Drivers\Ndis.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19030
```

Impact

Successful exploitation will allow an attacker to gain elevated privileges on a targeted system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1

Vulnerability Insight
The error exists as NDIS fails to check the length of a buffer prior to copying memory into it.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows NDIS Elevation of Privilege Vulnerability (3101722)`
OID:1.3.6.1.4.1.25623.1.0.806615
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-6098
url: https://support.microsoft.com/en-us/kb/3101722
url: https://technet.microsoft.com/library/security/MS15-117
cert-bund: CB-K15/1649
dfn-cert: DFN-CERT-2015-1742
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2876315)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-076.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to gain escalated privileges, read arbitrary kernel memory and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows XP x32 Edition Service Pack 3 and prior

. . . continues on next page . . .

... continued from previous page ...

- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

Multiple flaws are due to error related to multiple fetch within the kernel-mode driver (win32k.sys).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2876.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.902994

Version used: `2022-07-26T10:10:42Z`

References

```
cve: CVE-2013-1341
cve: CVE-2013-1342
cve: CVE-2013-1343
cve: CVE-2013-1344
cve: CVE-2013-3864
cve: CVE-2013-3865
cve: CVE-2013-3866
url: http://support.microsoft.com/kb/2876315
url: http://www.securityfocus.com/bid/62180
url: http://www.securityfocus.com/bid/62193
url: http://www.securityfocus.com/bid/62195
url: http://www.securityfocus.com/bid/62196
url: http://www.securityfocus.com/bid/62197
url: http://www.securityfocus.com/bid/62198
url: http://www.securityfocus.com/bid/62199
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-076
cert-bund: CB-K13/0638
dfn-cert: DFN-CERT-2013-1634
```

High (CVSS: 7.2)
NVT: Microsoft Windows Task Management Privilege Elevation Vulnerabilities (3089657)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-102.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Schedsvc.dll
```

... continues on next page ...

... continued from previous page ...

```
File version:     6.1.7601.17514
Vulnerable range: Version Less than  6.1.7601.18951
```

Impact

Successful exploitation will allow attacker to gain elevated privileges to perform arbitrary administration functions such as add users and install applications on the targeted machine.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

Multiple flaws are due to:
- Task Management failing to validate and enforce impersonation levels.
- Task Scheduler failing to properly verify certain file system interactions.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Task Management Privilege Elevation Vulnerabilities (3089657)`

OID:1.3.6.1.4.1.25623.1.0.806045

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2524
cve: CVE-2015-2525
cve: CVE-2015-2528
url: https://support.microsoft.com/en-us/kb/3082089
url: https://support.microsoft.com/en-us/kb/3084135
url: https://technet.microsoft.com/library/security/MS15-102
cert-bund: CB-K15/1321
dfn-cert: DFN-CERT-2015-1385
```

High (CVSS: 7.2)
NVT: Microsoft Windows Client/Server Run-time Subsystem Privilege Escalation Vulnerability (2790113)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-019.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to gain escalated privileges and execute the code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 Edition Service Pack 1 and prior

Vulnerability Insight
The flaw is due to an error in the Client/Server Run-time Subsystem (CSRSS) when handling the reference counter for certain objects in memory and can be execute code with escalated privileges.

Vulnerability Detection Method
Details: `Microsoft Windows Client/Server Run-time Subsystem Privilege Escalation Vulnera.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902946
Version used: `2022-07-26T10:10:42Z`

References

```
cve: CVE-2013-0076
url: http://support.microsoft.com/kb/2790113
url: http://www.securityfocus.com/bid/57821
url: http://www.securitytracker.com/id/1028127
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-019
dfn-cert: DFN-CERT-2013-0296
```

High (CVSS: 7.2)
NVT: Microsoft Windows Ancillary Function Driver Elevation of Privilege Vulnerability (2975684)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing a critical security update according to Microsoft Bulletin MS14-040.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to gain elevated privileges and execute arbitrary code and take complete control of an affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32 Service Pack 3 and prior
- Microsoft Windows 2003 x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight

Flaw is due to a double-free error in the Ancillary Function Driver within 'afd.sys'.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Ancillary Function Driver Elevation of Privilege Vulnerabilit.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.804671

Version used: `2023-07-27T05:05:08Z`

References

```
cve: CVE-2014-1767
url: https://support.microsoft.com/kb/2961072
url: http://www.securityfocus.com/bid/68394
url: https://support.microsoft.com/kb/2973408
url: https://technet.microsoft.com/library/security/ms14-040
cert-bund: CB-K14/0838
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (2731847)

Summary
This host is missing an important security update according to Microsoft Bulletin MS12-055.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to execute arbitrary code with kernel-mode privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
The flaw is due to a use-after-free error in win32k.sys when accessing objects in memory.

Vulnerability Detection Method
Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (273184.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903035
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-2527
url: http://support.microsoft.com/kb/2731847
url: http://www.securityfocus.com/bid/54873
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-055
dfn-cert: DFN-CERT-2012-1570
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (2778930)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-005.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow remote attackers to gain escalated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
The flaw is due to an error in 'win32k.sys' when handling window broadcast messages.

Vulnerability Detection Method
Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerability (2777893.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902938
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2013-0008
url: http://support.microsoft.com/kb/2778930
url: http://www.securityfocus.com/bid/57135
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-005
dfn-cert: DFN-CERT-2013-0045
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel Local Privilege Escalation Vulnerabilities (2880430)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-101

Vulnerability Detection Result
`The target host was found to be vulnerable`

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to cause a DoS (Denial of Service) and gain escalated privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows XP x32 Service Pack 3 and prior
- Microsoft Windows XP x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight

Multiple flaws are due to:

- An error within the win32k.sys driver can be exploited to corrupt memory.
- A use-after-free error exists within the win32k.sys driver.
- An error when processing TrueType font files can be exploited to cause a crash.
- A double fetch error exists within the portcls.sys driver.
- An integer overflow error exists within the win32k.sys driver.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel Local Privilege Escalation Vulnerabilities (2880430)`

OID:1.3.6.1.4.1.25623.1.0.903417

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-3899
cve: CVE-2013-3902
cve: CVE-2013-3903
cve: CVE-2013-3907
cve: CVE-2013-5058
url: http://support.microsoft.com/kb/2893984
url: http://www.securityfocus.com/bid/64080
url: http://www.securityfocus.com/bid/64084
url: http://www.securityfocus.com/bid/64087
url: http://www.securityfocus.com/bid/64090
url: http://www.securityfocus.com/bid/64091
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://support.microsoft.com/kb/2887069
url: http://www.securitytracker.com/id/1029461
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-101
cert-bund: CB-K13/1027
dfn-cert: DFN-CERT-2013-2048
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Escalation Vulnerability (2913602)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-003

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to gain escalated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
The flaw is due to the improper use of window handle thread-owned objects in memory. This may allow local attacker to gain elevated privileges.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel-Mode Drivers Privilege Escalation Vulnerability (29136.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903424
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2014-0262
url: https://support.microsoft.com/kb/2913602
url: http://www.securityfocus.com/bid/64725
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-003
cert-bund: CB-K14/0048
```

High (CVSS: 7.2)
NVT: Microsoft Windows Privilege Elevation Vulnerabilities (3096447)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-111.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Ntoskrnl.exe
File version:     6.1.7601.18741
Vulnerable range: Version Less than - 6.1.7601.19018
```

Impact
Successful exploitation will allow local users to gain privileges via a crafted application.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Multiple flaws are due to windows kernel is not handling objects in memory properly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Privilege Elevation Vulnerabilities (3096447)`
OID:1.3.6.1.4.1.25623.1.0.805762
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2549
cve: CVE-2015-2550
cve: CVE-2015-2552
cve: CVE-2015-2553
cve: CVE-2015-2554
url: https://support.microsoft.com/kb/3088195
url: https://technet.microsoft.com/library/security/MS15-111
cert-bund: CB-K15/1507
dfn-cert: DFN-CERT-2015-1586
```

High (CVSS: 7.2)
NVT: Microsoft Windows Kernel Privilege Escalation Vulnerabilities (2930275)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-015.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to cause a DoS (Denial of Service) and gain escalated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows XP x32 Service Pack 3 and prior
- Microsoft Windows XP x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to an information disclosure and an elevation of privilege vulnerability because the Windows kernel-mode driver improperly handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel Privilege Escalation Vulnerabilities (2930275)`
OID:1.3.6.1.4.1.25623.1.0.804409
Version used: `2023-07-26T05:05:09Z`

References
```
cve: CVE-2014-0300
cve: CVE-2014-0323
url: https://support.microsoft.com/kb/2930275
url: http://www.securityfocus.com/bid/66003
url: http://www.securityfocus.com/bid/66007
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-015
cert-bund: CB-K14/0296
```

High (CVSS: 7.2)
NVT: Microsoft Windows Remote Procedure Call Privilege Elevation Vulnerability (3067505)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-076.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attacker to gain privileged access.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 2003 x32/x64 Service Pack 2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2

Vulnerability Insight
The flaw occurs when Windows RPC inadvertently allows DCE/RPC connection reflection.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Remote Procedure Call Privilege Elevation Vulnerability (3067.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.805921
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2370
url: https://support.microsoft.com/en-us/kb/3067505
url: https://technet.microsoft.com/en-us/library/security/MS15-076
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1060
```

High (CVSS: 7.2)
NVT: Microsoft Windows Prtition Manager Privilege Elevation Vulnerability (2690533)

... continues on next page ...

. . . continued from previous page . . .

Summary

This host is missing an important security update according to Microsoft Bulletin MS12-033.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow attackers to gain escalated privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 Service Pack 1 and prior
- Microsoft Windows Vista Service Pack 2 and prior
- Microsoft Windows Server 2008 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 Service Pack 1 and prior

Vulnerability Insight

The flaw is due to the way Windows Partition Manager (partmgr.sys) allocates objects in memory, when two or more processes or threads call Plug and Play (PnP) Configuration Manager functions at the same time.

Vulnerability Detection Method

Details: `Microsoft Windows Prtition Manager Privilege Elevation Vulnerability (2690533)`

OID:1.3.6.1.4.1.25623.1.0.902677

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-0178
url: http://support.microsoft.com/kb/2690533
url: http://www.securityfocus.com/bid/53378
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-033
dfn-cert: DFN-CERT-2012-0894
```

High (CVSS: 7.2)

NVT: Microsoft ATM Font Driver Privilege Elevation Vulnerability (3077657)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-077.

Vulnerability Detection Result

```
Installed version: 5.1.2.230
```

. . . continues on next page . . .

... continued from previous page ...

```
Fixed version:     5.1.2.242
Installation
path / port:       C:\Windows
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code with kernel-mode privileges and take complete control of the affected system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight

An elevation of privilege vulnerability exists in Adobe Type Manager Font Driver (ATMFD) when it fails to properly handle objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft ATM Font Driver Privilege Elevation Vulnerability (3077657)`

OID:1.3.6.1.4.1.25623.1.0.805073

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2387
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3077657
url: http://www.securityfocus.com/bid/75587
url: https://technet.microsoft.com/library/security/MS15-077
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1060
```

High (CVSS: 7.2)
NVT: Microsoft Windows Shell Handler Privilege Escalation Vulnerability (2962488)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-027.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to gain elevated privileges and execute code in the context of the LocalSystem account.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
Flaw is due to an error in the 'ShellExecute' function within the Windows Shell API when handling file associations.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Shell Handler Privilege Escalation Vulnerability (2962488)`
OID:1.3.6.1.4.1.25623.1.0.804295
Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-1807
url: https://support.microsoft.com/kb/2926765
url: http://www.securityfocus.com/bid/67276
url: https://support.microsoft.com/kb/2962123
url: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2014/ms
↪14-027
cert-bund: CB-K14/0568
```

High (CVSS: 7.1)
NVT: Microsoft DirectAccess Security Advisory (2862152)

Summary
This host is missing an important security update according to Microsoft advisory (2862152).

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow an attacker to intercept the target user's network traffic and potentially determine their encrypted domain credentials.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows 8.1 x32/x64

Vulnerability Insight
The flaw is due to improper verification of DirectAccess server connections to DirectAccess clients by DirectAccess.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft DirectAccess Security Advisory (2862152)`
OID:1.3.6.1.4.1.25623.1.0.804143
Version used: `2023-07-27T05:05:08Z`

References
```
cve: CVE-2013-3876
url: http://www.securityfocus.com/bid/63666
url: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2014/2
↪862152
```

High (CVSS: 7.1)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2829996)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-036.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to gain escalated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to:
- Improper handling of certain objects in kernel memory.
- Improper parsing of crafted OpenType font files.

Vulnerability Detection Method
Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2829.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903202
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-1283
cve: CVE-2013-1291
cve: CVE-2013-1292
cve: CVE-2013-1293
url: http://support.microsoft.com/kb/2808735
url: http://www.securityfocus.com/bid/58853
url: http://www.securityfocus.com/bid/58858
url: http://www.securityfocus.com/bid/58859
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/58860
url: http://www.securitytracker.com/id/1028402
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-036
dfn-cert: DFN-CERT-2013-0748
```

High (CVSS: 7.1)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2829996)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-036.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to gain escalated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to:
- Improper handling of certain objects in kernel memory.
- Improper parsing of crafted OpenType font files.

Vulnerability Detection Method
Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2829.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903202
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-1283
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-1291
cve: CVE-2013-1292
cve: CVE-2013-1293
url: http://support.microsoft.com/kb/2808735
url: http://www.securityfocus.com/bid/58853
url: http://www.securityfocus.com/bid/58858
url: http://www.securityfocus.com/bid/58859
url: http://www.securityfocus.com/bid/58860
url: http://www.securitytracker.com/id/1028402
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-036
dfn-cert: DFN-CERT-2013-0748
```

High (CVSS: 7.1)
NVT: Microsoft Window XML Core Services Information Disclosure Vulnerability (2916036)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-005.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to read files on the local file system of the user or read content of web domains where the user is currently authenticated.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
The flaw is due to an unspecified error which improperly enforce cross-domain policies.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Window XML Core Services Information Disclosure Vulnerability (291603.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.903510

Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2014-0266
url: https://support.microsoft.com/kb/2916036
url: http://www.securityfocus.com/bid/65407
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-005
cert-bund: CB-K14/0168
```

High (CVSS: 7.1)

NVT: Microsoft Windows Kernel-Mode Driver TrueType Font DoS Vulnerability (3002885)

Summary

This host is missing a moderate security update according to Microsoft Bulletin MS14-079.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow an attacker to conduct denial-of-service attack.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2

Vulnerability Insight

The flaw is due to an integer underflow error in the 'vFill_IFIMETRICS' function within the win32k.sys module when processing font files.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel-Mode Driver TrueType Font DoS Vulnerability (3002885)`
OID:1.3.6.1.4.1.25623.1.0.804878
Version used: `2023-07-27T05:05:08Z`

References

```
cve: CVE-2014-6317
url: https://support.microsoft.com/kb/3002885
url: http://www.securityfocus.com/bid/70949
url: https://technet.microsoft.com/library/security/MS14-079
cert-bund: CB-K14/1402
```

High (CVSS: 7.1)
NVT: Microsoft Windows Kernel-Mode Driver Denial of Service Vulnerability (2845690)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-049.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow attackers to cause a denial of service.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

The flaw is due to an integer overflow error within Windows TCP/IP driver when handling packets during TCP connection, which can be exploited to cause the system to stop responding.

Vulnerability Detection Method

Details: `Microsoft Windows Kernel-Mode Driver Denial of Service Vulnerability (2845690)`
OID:1.3.6.1.4.1.25623.1.0.902975
Version used: `2022-05-25T07:40:23Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2013-3138
url: http://www.securitytracker.com/id/1028655
url: http://www.securityfocus.com/bid/60358
url: http://support.microsoft.com/kb/2845690
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-049
dfn-cert: DFN-CERT-2013-1112
```

[return to 192.168.56.103]

2.1.2 High 9200/tcp

High (CVSS: 10.0)
NVT: Elasticsearch End of Life (EOL) Detection

Summary

The Elasticsearch version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result

```
The "Elasticsearch" version on the remote host has reached the end of life.
CPE:               cpe:/a:elastic:elasticsearch:1.1.1
Installed version: 1.1.1
EOL version:       1.1
EOL date:          2015-09-25
```

Impact

An EOL version of Elasticsearch is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

Solution type: VendorFix

Update Elasticsearch to a version that still receives technical support and updates.

Vulnerability Detection Method

Checks if an EOL version is present on the target host.

Details: `Elasticsearch End of Life (EOL) Detection`

OID:1.3.6.1.4.1.25623.1.0.113131

Version used: `2023-07-20T05:05:17Z`

References

```
url: https://www.elastic.co/support/eol
```

High (CVSS: 9.8)
NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities - Windows

Summary
Elasticsearch is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     1.6.1
```

Impact
Successful exploitation will allow remote attackers to execute code or read arbitrary files.

Solution:
Solution type: VendorFix
Update to Elasticsearch version 1.6.1, or later.

Affected Software/OS
Elasticsearch version 1.0.0 through 1.6.0 on Windows.

Vulnerability Insight
The Flaw is due to:
- an error in the snapshot API calls (CVE-2015-5531)
- an attack that can result in remote code execution (CVE-2015-5377).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Elasticsearch < 1.6.1 Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.808091
Version used: 2024-02-15T05:05:40Z

References

```
cve: CVE-2015-5531
cve: CVE-2015-5377
url: https://www.elastic.co/community/security/
url: http://www.securityfocus.com/bid/75935
url: http://www.securityfocus.com/archive/1/archive/1/536017/100/0/threaded
cert-bund: CB-K15/1118
dfn-cert: DFN-CERT-2015-1160
```

High (CVSS: 8.8)
NVT: Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability - Windows

Summary
Elasticsearch is prone to an information disclosure vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     5.6.12
```

Impact

Successful exploitation would allow an authenticated attacker to acquire valid login credentials.

Solution:

Solution type: VendorFix

Update to version 5.6.12 or 6.4.1 respectively.

Affected Software/OS

Elasticsearch versions through 5.6.11 and 6.0.0 through 6.4.0.

Vulnerability Insight

The _cluster/settings API, when queried, could leak sensitive configuration information such as passwords, tokens or usernames.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.113276

Version used: `2024-02-15T05:05:40Z`

References

```
cve: CVE-2018-3831
url: https://discuss.elastic.co/t/elastic-stack-6-4-1-and-5-6-12-security-update
↪/149035
url: https://www.elastic.co/community/security
dfn-cert: DFN-CERT-2020-1653
```

[return to 192.168.56.103]

2.1.3 High 21/tcp

High (CVSS: 7.5)
NVT: FTP Brute Force Logins Reporting

Summary

It was possible to login into the remote FTP server using weak/known credentials.

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
vagrant:vagrant
```

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices
Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: `FTP Brute Force Logins Reporting`
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: `2023-12-06T05:06:11Z`

References
```
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2001-1594
cve: CVE-2013-7404
cve: CVE-2017-8218
cve: CVE-2018-19063
cve: CVE-2018-19064
```

[return to 192.168.56.103]

2.1.4 High 3389/tcp

High (CVSS: 9.8)
NVT: Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)

Summary
Microsoft Windows Remote Desktop Services is prone to the remote code execution vulnerability known as 'BlueKeep'.

Vulnerability Detection Result

```
By sending a crafted request the RDP service answered with a 'MCS Disconnect Pro
↪vider Ultimatum PDU - 2.2.2.3' response which indicates that a RCE attack can
↪be executed.
```

Impact
Successful exploitation would allow an attacker to execute arbitrary code on the target system. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.
As a workaround enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2.
NOTE: After enabling NLA affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.

Affected Software/OS
- Microsoft Windows 7
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2003
- Microsoft Windows Vista and Microsoft Windows XP (including Embedded)

Vulnerability Insight
A remote code execution vulnerability exists in Remote Desktop Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction.
For an in-depth analysis and further technical insights and details please see the references.

Vulnerability Detection Method
Sends a specially crafted request to the target systems Remote Desktop Service via RDP and checks the response.
Details: `Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.108611

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2023-04-18T10:19:20Z

References

```
cve: CVE-2019-0708
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019
↪-0708
url: https://support.microsoft.com/help/4499164
url: https://support.microsoft.com/help/4499175
url: https://support.microsoft.com/help/4499149
url: https://support.microsoft.com/help/4499180
url: https://support.microsoft.com/help/4500331
url: https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updat
↪ing-remote-desktop-services-cve-2019-0708/
url: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-
↪2019-0708
url: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s
↪erver-2008-R2-and-2008/cc732713(v=ws.11)
url: http://www.securityfocus.com/bid/108273
url: http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Deskto
↪p-BlueKeep-Denial-Of-Service.html
url: https://www.malwaretech.com/2019/05/analysis-of-cve-2019-0708-bluekeep.html
url: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-
↪really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708
cert-bund: CB-K19/0415
dfn-cert: DFN-CERT-2019-0977
```

[return to 192.168.56.103]

2.1.5 High 3306/tcp

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.43, 8.x <= 8.0.34, 8.1.0 Security Update (cpuoct2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.5.20
Fixed version:     5.7.44
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.44, 8.0.35, 8.1.1 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.43 and prior, 8.x through 8.0.34 and 8.1.0.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.43, 8.x <= 8.0.34, 8.1.0 Security Update (cpuoct2023.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.151218
Version used: `2023-10-27T16:11:33Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2023-38545
cve: CVE-2023-22084
cve: CVE-2023-38546
url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL
advisory-id: cpuoct2023
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0893
cert-bund: WID-SEC-2024-0290
cert-bund: WID-SEC-2024-0178
cert-bund: WID-SEC-2024-0175
cert-bund: WID-SEC-2024-0123
cert-bund: WID-SEC-2024-0119
cert-bund: WID-SEC-2024-0110
cert-bund: WID-SEC-2023-2788
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2570
dfn-cert: DFN-CERT-2024-1601
dfn-cert: DFN-CERT-2024-1517
dfn-cert: DFN-CERT-2024-1188
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-1090
dfn-cert: DFN-CERT-2024-1025
dfn-cert: DFN-CERT-2024-0963
dfn-cert: DFN-CERT-2024-0869
dfn-cert: DFN-CERT-2024-0593
dfn-cert: DFN-CERT-2024-0454
dfn-cert: DFN-CERT-2024-0376
dfn-cert: DFN-CERT-2024-0220
dfn-cert: DFN-CERT-2024-0185
dfn-cert: DFN-CERT-2024-0184
dfn-cert: DFN-CERT-2024-0181
dfn-cert: DFN-CERT-2024-0133
dfn-cert: DFN-CERT-2024-0132
dfn-cert: DFN-CERT-2024-0127
dfn-cert: DFN-CERT-2024-0108
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3064
dfn-cert: DFN-CERT-2023-2988
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2819
dfn-cert: DFN-CERT-2023-2763
dfn-cert: DFN-CERT-2023-2681
dfn-cert: DFN-CERT-2023-2680
dfn-cert: DFN-CERT-2023-2643
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2475
dfn-cert: DFN-CERT-2023-2458
```

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a vulnerability in libcurl.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.41
Installation
path / port:       3306/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Update to version 5.7.41, 8.0.32 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.40 and prior and 8.0 through 8.0.31.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Win.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.149170
Version used: `2023-10-13T05:06:10Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2022-32221
cve: CVE-2022-35260
cve: CVE-2022-42915
cve: CVE-2022-42916
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL
advisory-id: cpujan2023
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1026
cert-bund: WID-SEC-2023-0296
cert-bund: WID-SEC-2023-0189
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-1862
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1636
dfn-cert: DFN-CERT-2023-1230
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0898
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0278
dfn-cert: DFN-CERT-2023-0216
dfn-cert: DFN-CERT-2023-0214
dfn-cert: DFN-CERT-2023-0157
dfn-cert: DFN-CERT-2023-0156
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2401
dfn-cert: DFN-CERT-2022-2400
dfn-cert: DFN-CERT-2022-2393
dfn-cert: DFN-CERT-2022-2391
```

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.36
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.36, 8.0.27 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.35 and prior and 8.0 through 8.0.26.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.117741

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2021-10-23T08:58:44Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2021-3711
cve: CVE-2021-22926
cve: CVE-2021-35604
cve: CVE-2021-35624
cve: CVE-2021-22922
cve: CVE-2021-22923
cve: CVE-2021-22924
cve: CVE-2021-22925
cve: CVE-2021-22945
cve: CVE-2021-22946
cve: CVE-2021-22947
cve: CVE-2021-3712
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixMSQL
advisory-id: cpuoct2021
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0556
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1821
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1030
cert-bund: WID-SEC-2023-0530
cert-bund: WID-SEC-2022-2354
cert-bund: WID-SEC-2022-2000
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1515
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1225
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0875
cert-bund: WID-SEC-2022-0874
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0673
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0602
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0400
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0101
cert-bund: WID-SEC-2022-0094
cert-bund: CB-K22/0473
cert-bund: CB-K22/0469
cert-bund: CB-K22/0316
cert-bund: CB-K22/0224
cert-bund: CB-K22/0077
cert-bund: CB-K22/0072
cert-bund: CB-K22/0062
cert-bund: CB-K22/0045
cert-bund: CB-K22/0030
cert-bund: CB-K22/0011
cert-bund: CB-K21/1268
cert-bund: CB-K21/1179
cert-bund: CB-K21/1161
cert-bund: CB-K21/1087
cert-bund: CB-K21/0994
cert-bund: CB-K21/0991
cert-bund: CB-K21/0969
cert-bund: CB-K21/0907
cert-bund: CB-K21/0897
cert-bund: CB-K21/0797
dfn-cert: DFN-CERT-2024-0573
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-0469
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-1215
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0867
dfn-cert: DFN-CERT-2022-0835
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0437
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0122
dfn-cert: DFN-CERT-2022-0120
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0052
dfn-cert: DFN-CERT-2022-0031
```

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to a vulnerability in InnoDB (zlib).

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.42
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.42, 8.0.32 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.31.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Win.`

. . . continues on next page . . .

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.149536
Version used: 2023-10-13T05:06:10Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2022-37434
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0122
cert-bund: WID-SEC-2024-0120
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1791
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-1031
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0140
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2023-0125
cert-bund: WID-SEC-2022-1888
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-0929
dfn-cert: DFN-CERT-2024-0998
dfn-cert: DFN-CERT-2024-0790
dfn-cert: DFN-CERT-2024-0125
dfn-cert: DFN-CERT-2023-3028
dfn-cert: DFN-CERT-2023-2816
dfn-cert: DFN-CERT-2023-2799
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0881
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0122
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2421
dfn-cert: DFN-CERT-2022-2415
dfn-cert: DFN-CERT-2022-2366
dfn-cert: DFN-CERT-2022-2365
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-2363
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-1841
dfn-cert: DFN-CERT-2022-1710
```

High (CVSS: 9.8)
NVT: Oracle Mysql Security Update (cpuoct2018 - 02) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See reference
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle MySQL version 5.5.x through 5.5.61, 5.6.x through 5.6.41, 5.7.x through 5.7.23 and 8.0.x through 8.0.12.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to:

- An unspecified error within 'InnoDB (zlib)' component of MySQL Server.
- An unspecified error within 'Server: Parser' component of MySQL Server.
- An unspecified error within 'Client programs' component of MySQL Server.
- An unspecified error within 'Server: Storage Engines' component of MySQL Server.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Update (cpuoct2018 - 02) - Windows`
OID:1.3.6.1.4.1.25623.1.0.814258
Version used: `2022-06-24T09:38:38Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2018-3133
cve: CVE-2018-3174
cve: CVE-2018-3282
cve: CVE-2016-9843
cve: CVE-2016-9840
cve: CVE-2016-9841
cve: CVE-2016-9842
url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixMSQL
advisory-id: cpuoct2018
cert-bund: WID-SEC-2024-1232
cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/0714
cert-bund: CB-K18/1005
cert-bund: CB-K18/0799
cert-bund: CB-K18/0030
cert-bund: CB-K17/2199
cert-bund: CB-K17/2168
cert-bund: CB-K17/1745
cert-bund: CB-K17/1709
cert-bund: CB-K17/1622
cert-bund: CB-K17/1585
cert-bund: CB-K17/1062
cert-bund: CB-K17/0877
cert-bund: CB-K17/0784
cert-bund: CB-K16/1996
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-0998
dfn-cert: DFN-CERT-2020-1536
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0592
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-2273
dfn-cert: DFN-CERT-2018-2110
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-0659
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1825
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1655
dfn-cert: DFN-CERT-2017-1097
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
```

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.5.52 / 5.6 <= 5.6.33 / 5.7 <= 5.7.15 Security Update (cpuoct2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation of this vulnerability will allow a remote user to access restricted data.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.52 and prior, 5.6 through 5.6.33 and 5.7 through 5.7.15.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in the 'Server: Security: Encryption' and 'Server: Logging' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.52 / 5.6 <= 5.6.33 / 5.7 <= 5.7.15 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809386
Version used: `2021-10-13T11:01:26Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-5584
cve: CVE-2016-6662
cve: CVE-2016-7440
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
url: http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution
↪-Privesc-CVE-2016-6662.txt
url: https://www.exploit-db.com/exploits/40360/
cert-bund: CB-K17/0139
cert-bund: CB-K17/0055
cert-bund: CB-K16/1846
cert-bund: CB-K16/1755
cert-bund: CB-K16/1742
cert-bund: CB-K16/1714
cert-bund: CB-K16/1655
cert-bund: CB-K16/1624
cert-bund: CB-K16/1448
cert-bund: CB-K16/1392
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2017-0138
dfn-cert: DFN-CERT-2017-0060
```

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.39
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.39, 8.0.30 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.38 and prior and 8.0 through 8.0.29.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.148511

Version used: `2022-07-22T10:11:18Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2022-1292
cve: CVE-2022-27778
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-25032
cve: CVE-2022-21515
url: https://www.oracle.com/security-alerts/cpujul2022.html#AppendixMSQL
advisory-id: cpujul2022
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2723
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-1784
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0141
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1775
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0755
cert-bund: WID-SEC-2022-0736
cert-bund: WID-SEC-2022-0735
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0554
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0277
cert-bund: WID-SEC-2022-0071
cert-bund: WID-SEC-2022-0005
cert-bund: CB-K22/0619
cert-bund: CB-K22/0570
cert-bund: CB-K22/0536
cert-bund: CB-K22/0386
dfn-cert: DFN-CERT-2024-0998
dfn-cert: DFN-CERT-2024-0790
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-3028
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2600
dfn-cert: DFN-CERT-2023-2599
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0121
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2668
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2309
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2094
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2066
dfn-cert: DFN-CERT-2022-2059
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1992
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1875
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1614
dfn-cert: DFN-CERT-2022-1609
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1476
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1310
dfn-cert: DFN-CERT-2022-1304
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1049
dfn-cert: DFN-CERT-2022-0986
dfn-cert: DFN-CERT-2022-0768
dfn-cert: DFN-CERT-2022-0716
```

High (CVSS: 9.0)
NVT: Oracle MySQL Server Multiple Vulnerabilities - 01 - (Nov 2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data and cause a DoS (Denial of Service).

Solution:

Solution type: VendorFix

Apply the patch from the referenced vendor advisory or upgrade to the latest version.

Affected Software/OS

Oracle MySQL version 5.1.x to 5.1.64 and Oracle MySQL version 5.5.x to 5.5.26 on Windows.

Vulnerability Insight

The flaws are due to multiple unspecified errors in MySQL server component related to server replication, information schema, protocol and server optimizer.

Vulnerability Detection Method

Details: `Oracle MySQL Server Multiple Vulnerabilities - 01 - (Nov 2012) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803111
Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-3197
cve: CVE-2012-3163
cve: CVE-2012-3158
cve: CVE-2012-3150
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/55990
url: http://www.securityfocus.com/bid/56005
url: http://www.securityfocus.com/bid/56017
url: http://www.securityfocus.com/bid/56036
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
cert-bund: CB-K13/0919
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2012-2200
dfn-cert: DFN-CERT-2012-2118
```

High (CVSS: 8.1)
NVT: Oracle MySQL Server <= 5.7.34 / 8.0 <= 8.0.25 Security Update (cpujul2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.35
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.35, 8.0.26 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.34 and prior and 8.0 through 8.0.25.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.34 / 8.0 <= 8.0.25 Security Update (cpujul2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.146355
Version used: `2023-10-20T16:09:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2021-22901
cve: CVE-2019-17543
cve: CVE-2021-2389
cve: CVE-2021-2390
cve: CVE-2021-2356
cve: CVE-2021-2385
cve: CVE-2021-2342
cve: CVE-2021-2372
cve: CVE-2021-22897
cve: CVE-2021-22898
url: https://www.oracle.com/security-alerts/cpujul2021.html#AppendixMSQL
advisory-id: cpujul2021
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1963
cert-bund: WID-SEC-2022-0873
cert-bund: CB-K22/0044
cert-bund: CB-K21/0813
cert-bund: CB-K21/0770
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2019-2216
```

High (CVSS: 8.1)
NVT: Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (cpu-jul2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Oracle MySQL Server versions 5.5.49 and prior, 5.6 through 5.6.30 and 5.7 through 5.7.12.

Vulnerability Insight

Multiple unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.808588

Version used: `2023-11-03T05:05:46Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-3477
cve: CVE-2016-3521
cve: CVE-2016-3615
cve: CVE-2016-5440
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91902
url: http://www.securityfocus.com/bid/91932
url: http://www.securityfocus.com/bid/91960
url: http://www.securityfocus.com/bid/91953
advisory-id: cpujul2016
cert-bund: CB-K16/1755
cert-bund: CB-K16/1742
cert-bund: CB-K16/1448
cert-bund: CB-K16/1146
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
```

High (CVSS: 7.7)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to have impact on availability, confidentiality and integrity.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier, 5.7.17 and earlier on Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to multiple unspecified errors in the 'Server: DML', 'Server: Optimizer', 'Server: Thread Pooling', 'Client mysqldump', 'Server: Security: Privileges' components of the application.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.810882
Version used: `2023-11-03T05:05:46Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2017-3309
cve: CVE-2017-3308
cve: CVE-2017-3329
cve: CVE-2017-3456
cve: CVE-2017-3453
cve: CVE-2017-3600
cve: CVE-2017-3462
cve: CVE-2017-3463
cve: CVE-2017-3461
cve: CVE-2017-3464
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97742
url: http://www.securityfocus.com/bid/97725
url: http://www.securityfocus.com/bid/97763
url: http://www.securityfocus.com/bid/97831
url: http://www.securityfocus.com/bid/97776
url: http://www.securityfocus.com/bid/97765
url: http://www.securityfocus.com/bid/97851
url: http://www.securityfocus.com/bid/97849
url: http://www.securityfocus.com/bid/97812
url: http://www.securityfocus.com/bid/97818
cert-bund: CB-K18/0224
cert-bund: CB-K17/1732
cert-bund: CB-K17/1604
cert-bund: CB-K17/1563
cert-bund: CB-K17/1401
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0927
cert-bund: CB-K17/0657
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1630
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0959
dfn-cert: DFN-CERT-2017-0675
```

High (CVSS: 7.7)
NVT: Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

Apply the latest patch from vendor. Please see the references for more information.

Affected Software/OS

Oracle MySQL version 5.5.59 and earlier, 5.6.39 and earlier, 5.7.21 and earlier on Windows

Vulnerability Insight

Multiple flaws exist due to

- Multiple errors in the 'Client programs' component of MySQL Server.

. . . continues on next page . . .

. . . continued from previous page . . .

- An error in the 'Server: Locking' component of MySQL Server.
- An error in the 'Server: Optimizer' component of MySQL Server.
- Multiple errors in the 'Server: DDL' component of MySQL Server.
- Multiple errors in the 'Server: Replication' component of MySQL Server.
- An error in the 'InnoDB' component of MySQL Server.
- An error in the 'Server : Security : Privileges' component of MySQL Server.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.813148
Version used: `2024-02-29T14:37:57Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2018-2761
cve: CVE-2018-2771
cve: CVE-2018-2781
cve: CVE-2018-2773
cve: CVE-2018-2817
cve: CVE-2018-2813
cve: CVE-2018-2755
cve: CVE-2018-2819
cve: CVE-2018-2818
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1594
cert-bund: CB-K18/0608
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0913
dfn-cert: DFN-CERT-2018-0723
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.5.39 / 5.6 <= 5.6.20 Security Update (cpuoct2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.40
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:
Solution type: VendorFix
Update to version 5.5.40, 5.6.21 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5.39 and prior and 5.6 through 5.6.20.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to C API SSL CERTIFICATE HANDLING, SERVER:DML, SERVER:SSL:yaSSL, SERVER:OPTIMIZER, SERVER:INNODB DML FOREIGN KEYS.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.39 / 5.6 <= 5.6.20 Security Update (cpuoct2014) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804781
Version used: `2022-04-14T11:24:11Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2014-6507
cve: CVE-2014-6491
cve: CVE-2014-6500
cve: CVE-2014-6469
cve: CVE-2014-6555
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-6559
cve: CVE-2014-6494
cve: CVE-2014-6496
cve: CVE-2014-6464
url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL
url: http://www.securityfocus.com/bid/70444
url: http://www.securityfocus.com/bid/70446
url: http://www.securityfocus.com/bid/70451
url: http://www.securityfocus.com/bid/70469
url: http://www.securityfocus.com/bid/70478
url: http://www.securityfocus.com/bid/70487
url: http://www.securityfocus.com/bid/70497
url: http://www.securityfocus.com/bid/70530
url: http://www.securityfocus.com/bid/70550
advisory-id: cpuoct2014
cert-bund: CB-K15/1518
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K14/1482
cert-bund: CB-K14/1420
cert-bund: CB-K14/1299
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpuoct2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.43
Installation
path / port:       3306/tcp
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Update to version 5.7.43, 8.0.34 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.33.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpuoct2023) - Win.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.151214
Version used: `2023-10-20T05:06:03Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2023-2650
cve: CVE-2023-0464
cve: CVE-2023-0465
cve: CVE-2023-0466
cve: CVE-2023-1255
url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL
advisory-id: cpuoct2023
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0120
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2024-0053
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2674
cert-bund: WID-SEC-2023-1794
cert-bund: WID-SEC-2023-1781
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1323
cert-bund: WID-SEC-2023-1130
cert-bund: WID-SEC-2023-1053
cert-bund: WID-SEC-2023-0782
cert-bund: WID-SEC-2023-0732
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0565
dfn-cert: DFN-CERT-2024-0147
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-0125
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3070
dfn-cert: DFN-CERT-2023-2749
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1903
dfn-cert: DFN-CERT-2023-1720
dfn-cert: DFN-CERT-2023-1649
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1428
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1332
dfn-cert: DFN-CERT-2023-1246
dfn-cert: DFN-CERT-2023-1245
dfn-cert: DFN-CERT-2023-1233
dfn-cert: DFN-CERT-2023-0999
dfn-cert: DFN-CERT-2023-0960
dfn-cert: DFN-CERT-2023-0929
dfn-cert: DFN-CERT-2023-0904
dfn-cert: DFN-CERT-2023-0782
dfn-cert: DFN-CERT-2023-0700
dfn-cert: DFN-CERT-2023-0645
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpuapr2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.42
Installation
path / port:       3306/tcp
```

Solution:

. . . continues on next page . . .

... continued from previous page ...

Solution type: VendorFix
Update to version 5.7.42, 8.0.33 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.32.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpuapr2023) - Win.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.149538
Version used: `2023-10-13T05:06:10Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2023-0215
cve: CVE-2022-43551
cve: CVE-2023-21980
cve: CVE-2022-4304
cve: CVE-2022-4450
cve: CVE-2023-0286
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0114
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1886
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1793
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1553
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0777
cert-bund: WID-SEC-2023-0304
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-2375
dfn-cert: DFN-CERT-2024-1188
dfn-cert: DFN-CERT-2024-0593
dfn-cert: DFN-CERT-2024-0454
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0126
dfn-cert: DFN-CERT-2024-0016
dfn-cert: DFN-CERT-2023-2192
dfn-cert: DFN-CERT-2023-1760
dfn-cert: DFN-CERT-2023-1697
dfn-cert: DFN-CERT-2023-1656
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1522
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1256
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-1043
dfn-cert: DFN-CERT-2023-1037
dfn-cert: DFN-CERT-2023-0898
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0774
dfn-cert: DFN-CERT-2023-0685
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0639
dfn-cert: DFN-CERT-2023-0618
dfn-cert: DFN-CERT-2023-0543
dfn-cert: DFN-CERT-2023-0471
dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0329
dfn-cert: DFN-CERT-2023-0318
dfn-cert: DFN-CERT-2023-0310
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0288
dfn-cert: DFN-CERT-2023-0284
dfn-cert: DFN-CERT-2023-0283
dfn-cert: DFN-CERT-2022-2902
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.30 Security Update (cpuapr2023) - Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.42
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.42, 8.0.31 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.30.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.30 Security Update (cpuapr2023) - Win.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.149534

Version used: `2023-10-13T05:06:10Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2023-21912
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1033
dfn-cert: DFN-CERT-2023-1058
dfn-cert: DFN-CERT-2023-1037
dfn-cert: DFN-CERT-2023-0885
```

High (CVSS: 7.5)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to cause the affected application to crash, resulting in a denial-of-service condition.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.54 and earlier, 5.6.20 and earlier on Windows

Vulnerability Insight

The flaw exists due to some unspecified error in the 'Server: C API' component due to failure to handle exceptional conditions.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows`

OID:1.3.6.1.4.1.25623.1.0.810880

Version used: `2023-07-14T16:09:27Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

`cve: CVE-2017-3302`

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/96162
cert-bund: CB-K18/0224
cert-bund: CB-K17/1604
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/0657
cert-bund: CB-K17/0423
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0430
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.37 / 8.0 <= 8.0.28 Security Update (cpuapr2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.38
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.38, 8.0.29 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.37 and prior and 8.0 through 8.0.28.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.37 / 8.0 <= 8.0.28 Security Update (cpuapr2022) - Wi.`
`↪..`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.113944
Version used: 2022-04-25T14:30:15Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2022-0778
cve: CVE-2022-21454
cve: CVE-2022-21417
cve: CVE-2022-21427
cve: CVE-2022-21451
cve: CVE-2022-21444
cve: CVE-2022-21460
url: https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixMSQL
advisory-id: cpuapr2022
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1081
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0551
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0270
cert-bund: WID-SEC-2022-0261
cert-bund: WID-SEC-2022-0200
cert-bund: WID-SEC-2022-0190
cert-bund: WID-SEC-2022-0169
cert-bund: WID-SEC-2022-0065
cert-bund: CB-K22/0619
cert-bund: CB-K22/0470
cert-bund: CB-K22/0468
cert-bund: CB-K22/0321
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-0081
dfn-cert: DFN-CERT-2022-2668
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2094
dfn-cert: DFN-CERT-2022-2059
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1928
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1667
dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1370
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1205
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-0955
dfn-cert: DFN-CERT-2022-0902
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0759
dfn-cert: DFN-CERT-2022-0627
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0610
dfn-cert: DFN-CERT-2022-0603
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.37
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.37, 8.0.28 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.36 and prior and 8.0 through 8.0.27.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.147465
Version used: `2023-10-19T05:05:21Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2021-22946
cve: CVE-2022-21367
cve: CVE-2022-21270
cve: CVE-2022-21304
cve: CVE-2022-21344
cve: CVE-2022-21303
cve: CVE-2022-21245
cve: CVE-2021-22947
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixMSQL
advisory-id: cpujan2022
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0875
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0101
cert-bund: CB-K22/0316
cert-bund: CB-K22/0077
cert-bund: CB-K22/0062
cert-bund: CB-K22/0030
cert-bund: CB-K21/0991
cert-bund: CB-K21/0969
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-0835
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0052
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.34
Installation
path / port:       3306/tcp
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Update to version 5.7.34, 8.0.24 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.33 and prior and 8.0 through 8.0.23.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145796
Version used: `2023-10-20T16:09:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2021-3449
cve: CVE-2021-3450
cve: CVE-2021-23840
cve: CVE-2021-23841
cve: CVE-2021-2307
cve: CVE-2021-2304
cve: CVE-2021-2180
cve: CVE-2021-2194
cve: CVE-2021-2166
cve: CVE-2021-2179
cve: CVE-2021-2226
cve: CVE-2021-2169
cve: CVE-2021-2146
cve: CVE-2021-2174
cve: CVE-2021-2171
cve: CVE-2021-2162
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0065
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1320
cert-bund: WID-SEC-2022-1303
cert-bund: WID-SEC-2022-1294
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0671
cert-bund: WID-SEC-2022-0669
cert-bund: WID-SEC-2022-0602
cert-bund: CB-K22/0476
cert-bund: CB-K22/0061
cert-bund: CB-K21/1097
cert-bund: CB-K21/1095
cert-bund: CB-K21/1065
cert-bund: CB-K21/0785
cert-bund: CB-K21/0770
cert-bund: CB-K21/0573
cert-bund: CB-K21/0572
cert-bund: CB-K21/0565
cert-bund: CB-K21/0421
cert-bund: CB-K21/0412
cert-bund: CB-K21/0409
cert-bund: CB-K21/0389
cert-bund: CB-K21/0317
cert-bund: CB-K21/0185
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0024
```

High (CVSS: 7.5)
NVT: Oracle MySQL Denial Of Service Vulnerability (Feb 2017) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.21
Installation
path / port:       3306/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation of this vulnerability will allow attackers to cause crash of applications using that MySQL client.

Solution:
Solution type: VendorFix
Upgrade to Oracle MySQL version 5.6.21 or 5.7.5 or later.

Affected Software/OS
Oracle MySQL version before 5.6.21 and 5.7.x before 5.7.5 on Windows

Vulnerability Insight
Multiple errors exist as,
- In sql-common/client.c script 'mysql_prune_stmt_list' function, the for loop adds elements to pruned_list without removing it from the existing list.
- If application gets disconnected just before it tries to prepare a new statement, 'mysql_prune_stmt_list' tries to detach all previously prepared statements.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Denial Of Service Vulnerability (Feb 2017) - Windows`
OID:1.3.6.1.4.1.25623.1.0.810603
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2017-3302
url: https://bugs.mysql.com/bug.php?id=63363
url: https://bugs.mysql.com/bug.php?id=70429
url: http://www.openwall.com/lists/oss-security/2017/02/11/11
cert-bund: CB-K18/0224
cert-bund: CB-K17/1604
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/0657
cert-bund: CB-K17/0423
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0430
```

High (CVSS: 7.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-01 (Feb 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
```

Impact

Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server version 5.5.40 and earlier, and 5.6.21 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Server:-Security:Encryption, InnoDB:DML, Replication, and Security:Privileges:Foreign Key.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-01 (Feb 2015) - Windows`
OID:1.3.6.1.4.1.25623.1.0.805132
Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2015-0411
cve: CVE-2014-6568
cve: CVE-2015-0382
cve: CVE-2015-0381
cve: CVE-2015-0374
url: http://secunia.com/advisories/62525
url: http://www.securityfocus.com/bid/72191
url: http://www.securityfocus.com/bid/72210
url: http://www.securityfocus.com/bid/72200
url: http://www.securityfocus.com/bid/72214
url: http://www.securityfocus.com/bid/72227
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/1193
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.6.48 Security Update (cpujul2020) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.49
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.6.49 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle MySQL Server versions 5.6.48 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.48 Security Update (cpujul2020) - Windows`
OID:1.3.6.1.4.1.25623.1.0.144286
Version used: `2021-08-16T12:00:57Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2020-1967
cve: CVE-2020-14539
cve: CVE-2020-14559
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixMSQL
advisory-id: cpujul2020
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-3080
cert-bund: CB-K21/1088
cert-bund: CB-K21/0070
cert-bund: CB-K20/1023
cert-bund: CB-K20/1017
cert-bund: CB-K20/0711
cert-bund: CB-K20/0708
cert-bund: CB-K20/0357
dfn-cert: DFN-CERT-2020-2295
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1827
dfn-cert: DFN-CERT-2020-1788
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-0956
dfn-cert: DFN-CERT-2020-0930
dfn-cert: DFN-CERT-2020-0841
dfn-cert: DFN-CERT-2020-0824
dfn-cert: DFN-CERT-2020-0822
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujul2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Oracle MySQL Server versions 5.5.45 and prior and 5.6 through 5.6.26.

Vulnerability Insight

An unspecified error exists in the 'MySQL Server' component via unknown vectors related to the 'Option' sub-component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujul2016) - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.808591

Version used: `2022-07-07T10:16:06Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-3471
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91913
advisory-id: cpujul2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
```

High (CVSS: 7.2)
NVT: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpujan2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.46 and prior, 5.6 through 5.6.27 and version 5.7.9.

Vulnerability Insight
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpujan20.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.806876

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-0609
cve: CVE-2016-0608
cve: CVE-2016-0606
cve: CVE-2016-0600
cve: CVE-2016-0598
cve: CVE-2016-0597
cve: CVE-2016-0546
cve: CVE-2016-0505
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81258
url: http://www.securityfocus.com/bid/81226
url: http://www.securityfocus.com/bid/81188
url: http://www.securityfocus.com/bid/81182
url: http://www.securityfocus.com/bid/81151
url: http://www.securityfocus.com/bid/81066
url: http://www.securityfocus.com/bid/81088
advisory-id: cpujan2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133
cert-bund: CB-K16/0094
```

High (CVSS: 7.2)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-06 (Oct 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

. . . continues on next page . . .

... continued from previous page ...

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server Server 5.5.44 and earlier, and 5.6.25 and earlier

Vulnerability Insight

Unspecified errors exist in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-06 (Oct 2015) - Windows`

OID:1.3.6.1.4.1.25623.1.0.805769

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-4879
cve: CVE-2015-4819
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77140
url: http://www.securityfocus.com/bid/77196
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K15/1844
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638
```

High (CVSS: 7.2)
NVT: Oracle MySQL Server <= 5.7.29 / 8.0 <= 8.0.19 Security Update (cpuapr2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to a vulnerability in the parser.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.30
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.30, 8.0.20 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.29 and prior and 8.0 through 8.0.19.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.29 / 8.0 <= 8.0.19 Security Update (cpuapr2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145800
Version used: `2021-08-26T13:01:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2021-2144
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2023-0065
cert-bund: CB-K21/0421
```

High (CVSS: 7.2)
NVT: Oracle MySQL Unspecified Vulnerability-03 (Sep 2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.52
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an remote attacker to gain elevated privileges on the affected system, also could allow buffer overflow attacks.

Solution:

Solution type: VendorFix

Upgrade to Oracle MySQL Server 5.5.52 or later.

Affected Software/OS

Oracle MySQL Server 5.5.x to 5.5.51 on windows

Vulnerability Insight

Multiple errors exist. Please see the references for more information.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Unspecified Vulnerability-03 (Sep 2016) - Windows`

OID:1.3.6.1.4.1.25623.1.0.809300

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

... continues on next page ...

. . . continued from previous page . . .

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
url: http://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-52.html
```

High (CVSS: 7.1)
NVT: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (cpujan2019) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.

Solution:

Solution type: VendorFix

Updates are available. Apply the necessary patch from the referenced link.

Affected Software/OS

Oracle MySQL Server versions 5.6.42 and prior, 5.7 through 5.7.24 and 8.0 through 8.0.13.

Vulnerability Insight

The attacks range in variety and difficulty. Most of them allow an attacker with network access via multiple protocols to compromise the MySQL Server.

For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.112489

Version used: `2023-02-02T10:09:00Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2019-2534
cve: CVE-2019-2529
cve: CVE-2019-2482
cve: CVE-2019-2455
cve: CVE-2019-2503
cve: CVE-2018-0734
cve: CVE-2019-2537
cve: CVE-2019-2481
cve: CVE-2019-2507
cve: CVE-2019-2531
cve: CVE-2018-5407
url: https://www.oracle.com/security-alerts/cpujan2019.html#AppendixMSQL
advisory-id: cpujan2019
cert-bund: WID-SEC-2023-3083
cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2022-1696
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0517
cert-bund: CB-K22/0045
cert-bund: CB-K20/0324
cert-bund: CB-K20/0136
cert-bund: CB-K19/1121
cert-bund: CB-K19/0696
cert-bund: CB-K19/0622
cert-bund: CB-K19/0615
cert-bund: CB-K19/0321
cert-bund: CB-K19/0320
cert-bund: CB-K19/0319
cert-bund: CB-K19/0318
cert-bund: CB-K19/0316
cert-bund: CB-K19/0314
cert-bund: CB-K19/0050
cert-bund: CB-K19/0044
cert-bund: CB-K18/1173
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/1065
cert-bund: CB-K18/1039
dfn-cert: DFN-CERT-2020-0326
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-2305
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1600
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1562
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0782
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0778
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0232
dfn-cert: DFN-CERT-2019-0204
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2019-0104
dfn-cert: DFN-CERT-2019-0103
dfn-cert: DFN-CERT-2019-0102
dfn-cert: DFN-CERT-2018-2541
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2513
dfn-cert: DFN-CERT-2018-2456
dfn-cert: DFN-CERT-2018-2444
dfn-cert: DFN-CERT-2018-2396
dfn-cert: DFN-CERT-2018-2360
dfn-cert: DFN-CERT-2018-2338
dfn-cert: DFN-CERT-2018-2214
```

High (CVSS: 7.1)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service attack and partially modify data.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.19 and earlier on Windows

Vulnerability Insight

The flaw exists due to an error in 'Server:Partition' component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.812650
Version used: `2024-02-29T14:37:57Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2018-2562
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0480
cert-bund: CB-K18/0392
cert-bund: CB-K18/0265
cert-bund: CB-K18/0096
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0424
dfn-cert: DFN-CERT-2018-0286
dfn-cert: DFN-CERT-2018-0101
```

High (CVSS: 7.0)
NVT: Oracle MySQL Server <= 5.5.51 / 5.6 <= 5.6.32 / 5.7 <= 5.7.14 Security Update (cpuoct2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation of these vulnerabilities will allow remote authenticated attackers to cause denial of service conditions and gain elevated privileges.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.51 and prior, 5.6 through 5.6.32 and 5.7 through 5.7.14.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple flaws exist due to multiple unspecified errors in the 'Server:GIS', 'Server:Federated', 'Server:Optimizer', 'Server:Types', 'Server:Error Handling' and 'Server:MyISAM' components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.5.51 / 5.6 <= 5.6.32 / 5.7 <= 5.7.14 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.809372

Version used: `2021-10-13T11:01:26Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-3492
cve: CVE-2016-5626
cve: CVE-2016-5629
cve: CVE-2016-5616
cve: CVE-2016-5617
cve: CVE-2016-8283
cve: CVE-2016-6663
cve: CVE-2016-6664
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K18/0224
cert-bund: CB-K17/1298
cert-bund: CB-K17/0139
cert-bund: CB-K16/1979
cert-bund: CB-K16/1846
cert-bund: CB-K16/1755
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0138
```

[return to 192.168.56.103]

2.1.6 High 8383/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

Solution:

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`

OID:1.3.6.1.4.1.25623.1.0.108031

Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`

. . . continues on next page . . .

... continued from previous page ...

Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

References

cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
```

[return to 192.168.56.103]

2.1.7 High 1617/tcp

High (CVSS: 7.5)
NVT: Java JMX Insecure Configuration Vulnerability

Summary
The Java JMX interface is configured in an insecure way by allowing unauthenticated attackers to load classes from any remote URL.

Vulnerability Detection Result

```
It was possible to call 'javax.management.remote.rmi.RMIServer.newClient' on the
↪ RMI port 49157/tcp without providing any credentials.
```

Solution:
Solution type: Mitigation
Enable password authentication and/or SSL client certificate authentication for the JMX agent.

Vulnerability Detection Method
Sends crafted RMI requests and checks the responses.
Details: `Java JMX Insecure Configuration Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.143207
Version used: `2020-11-10T09:46:51Z`

References

```
url: https://mogwailabs.de/blog/2019/04/attacking-rmi-based-jmx-services/
url: https://www.optiv.com/blog/exploiting-jmx-rmi
url: https://www.rapid7.com/db/modules/exploit/multi/misc/java_jmx_server
```

[return to 192.168.56.103]

2.1.8 High 80/tcp

High (CVSS: 10.0)
NVT: Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check

Product detection result

```
cpe:/a:microsoft:internet_information_services:7.5
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:
↪ 1.3.6.1.4.1.25623.1.0.900710)
```

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method
Sends a special crafted HTTP GET request and checks the response.
Details: `Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105257
Version used: `2023-11-10T16:09:31Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:7.5`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2015-1635
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/topic/ms15-034-vulnerability-in-http-sy
↪s-could-allow-remote-code-execution-april-14-2015-e8755c1e-c5a8-fa75-c7b1-3208
↪7b127850
url: https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2015/m
↪s15-034
url: http://pastebin.com/ypURDPc4
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545
```

[return to 192.168.56.103]

2.1.9 High 22/tcp

High (CVSS: 9.8)
NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

openssh is prone to a security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     7.2
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:

Solution type: VendorFix

Upgrade to OpenSSH version 7.2 or later.

Affected Software/OS

OpenSSH versions before 7.2 on Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

An access flaw was discovered in OpenSSH, It did not correctly handle failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X application could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forwarding was requested.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH X11 Forwarding Security Bypass Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.810768
Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
cve: CVE-2016-1908
url: http://openwall.com/lists/oss-security/2016/01/15/13
url: http://www.securityfocus.com/bid/84427
url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4
url: http://www.openssh.com/txt/release-7.2
url: https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0
↪db113c71e234416c
url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741
cert-bund: CB-K16/1485
cert-bund: CB-K16/0694
cert-bund: CB-K16/0684
cert-bund: CB-K16/0449
cert-bund: CB-K16/0162
dfn-cert: DFN-CERT-2018-1828
```

High (CVSS: 9.8)
NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary

It was possible to login into the remote SSH server using default credentials.

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
vagrant:vagrant
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight
As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `2024-03-15T05:06:15Z`

References

```
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2020-9473
cve: CVE-2023-1944
cve: CVE-2024-22902
```

High (CVSS: 7.8)
NVT: OpenSSH Multiple Vulnerabilities (Jan 2017) - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
openssh is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     7.4
Installation
path / port:       22/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.

Solution:

Solution type: VendorFix

Upgrade to OpenSSH version 7.4 or later.

Affected Software/OS

OpenSSH versions before 7.4 on Windows.

Vulnerability Insight

Multiple flaws exist due to:

- An 'authfile.c' script does not properly consider the effects of realloc on buffer contents.
- The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers.
- The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used.
- An untrusted search path vulnerability in ssh-agent.c in ssh-agent.
- NULL pointer dereference error due to an out-of-sequence NEWKEYS message.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `OpenSSH Multiple Vulnerabilities (Jan 2017) - Windows`

OID:1.3.6.1.4.1.25623.1.0.810325

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:7.1`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
cve: CVE-2016-10009
cve: CVE-2016-10010
cve: CVE-2016-10011
cve: CVE-2016-10012
cve: CVE-2016-10708
url: https://www.openssh.com/txt/release-7.4
url: http://www.securityfocus.com/bid/94968
url: http://www.securityfocus.com/bid/94972
url: http://www.securityfocus.com/bid/94977
url: http://www.securityfocus.com/bid/94975
url: http://www.openwall.com/lists/oss-security/2016/12/19/2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html
url: https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e93
↪3e6b931de1d16737
cert-bund: WID-SEC-2023-1996
cert-bund: CB-K18/0919
cert-bund: CB-K18/0591
cert-bund: CB-K18/0137
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1292
cert-bund: CB-K17/1061
cert-bund: CB-K17/0527
cert-bund: CB-K17/0377
cert-bund: CB-K17/0127
cert-bund: CB-K17/0041
cert-bund: CB-K16/1991
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-2259
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-2068
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1568
dfn-cert: DFN-CERT-2018-1432
dfn-cert: DFN-CERT-2018-1112
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-1068
dfn-cert: DFN-CERT-2018-0150
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-1096
dfn-cert: DFN-CERT-2017-0532
dfn-cert: DFN-CERT-2017-0386
dfn-cert: DFN-CERT-2017-0130
dfn-cert: DFN-CERT-2017-0042
```

High (CVSS: 7.5)
NVT: OpenSSH Denial of Service And User Enumeration Vulnerabilities - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

openssh is prone to denial of service and user enumeration vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     7.3
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.

Solution:

Solution type: VendorFix

Upgrade to OpenSSH version 7.3 or later.

Affected Software/OS

OpenSSH versions before 7.3 on Windows

Vulnerability Insight

Multiple flaws exist due to:

- The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication.
- The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `OpenSSH Denial of Service And User Enumeration Vulnerabilities - Windows`

OID:1.3.6.1.4.1.25623.1.0.809121

Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:7.1`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
cve: CVE-2016-6515
cve: CVE-2016-6210
url: http://www.openssh.com/txt/release-7.3
url: http://www.securityfocus.com/bid/92212
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://seclists.org/fulldisclosure/2016/Jul/51
url: https://security-tracker.debian.org/tracker/CVE-2016-6210
url: http://openwall.com/lists/oss-security/2016/08/01/2
cert-bund: WID-SEC-2023-0450
cert-bund: WID-SEC-2023-0449
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1753
cert-bund: CB-K17/1349
cert-bund: CB-K17/1292
cert-bund: CB-K17/0055
cert-bund: CB-K16/1837
cert-bund: CB-K16/1629
cert-bund: CB-K16/1487
cert-bund: CB-K16/1485
cert-bund: CB-K16/1252
cert-bund: CB-K16/1221
cert-bund: CB-K16/1082
dfn-cert: DFN-CERT-2023-1920
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1407
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-0060
```

[return to 192.168.56.103]

2.1.10 High 8009/tcp

High (CVSS: 9.8)
NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

Summary
Apache Tomcat is prone to a remote code execution vulnerability (dubbed 'Ghostcat') in the AJP connector.

Vulnerability Detection Result

```
It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.
Result:
AB v\x0004 Ã\x0088 \x0002OK  \x0003Â \x0007 =JSESSIONID=651CFF9C096BE49C6F9C880D
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪2D74FD1E; Path=/; HttpOnly Â \x0001 \x001Ctext/html;charset=ISO-8859-1 Â \x000
↪3 \x00041262 AB\x0004Ã²\x0003\x0004Ã®<?xml version="1.0" encoding="ISO-8859-1"
↪?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at
      http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">
  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>
</web-app>
 AB \x0002\x0005\x0001
```

Solution:

Solution type: VendorFix

Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on fixed versions.

Affected Software/OS

Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled. Other products like JBoss or Wildfly which are using Tomcat might be affected as well.

Vulnerability Insight

Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.

Vulnerability Detection Method

Sends a crafted AJP request and checks the response.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Apache Tomcat AJP RCE Vulnerability (Ghostcat)
OID:1.3.6.1.4.1.25623.1.0.143545
Version used: 2023-07-06T05:05:36Z

References

```
cve: CVE-2020-1938
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1
↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
url: https://www.chaitin.cn/en/ghostcat
url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487
url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi
url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances
↪-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/
url: https://tomcat.apache.org/tomcat-7.0-doc/changelog.html
url: https://tomcat.apache.org/tomcat-8.5-doc/changelog.html
url: https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2023-2480
cert-bund: CB-K20/0711
cert-bund: CB-K20/0705
cert-bund: CB-K20/0693
cert-bund: CB-K20/0555
cert-bund: CB-K20/0543
cert-bund: CB-K20/0154
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-1413
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2020-1134
dfn-cert: DFN-CERT-2020-0850
dfn-cert: DFN-CERT-2020-0835
dfn-cert: DFN-CERT-2020-0821
dfn-cert: DFN-CERT-2020-0569
dfn-cert: DFN-CERT-2020-0557
dfn-cert: DFN-CERT-2020-0501
dfn-cert: DFN-CERT-2020-0381
```

[return to 192.168.56.103]

2.1.11 High 8282/tcp

High (CVSS: 10.0)
NVT: Apache Axis2 Default Credentials (HTTP) - Active Check

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote Apache Axis2 web interface is using known default credentials.

Vulnerability Detection Result

```
It was possible to login at "http://192.168.56.103:8282/axis2/axis2-admin/" usin
↪g the following credentials (Username:Password):
 - admin:axis2
```

Impact

This issue may be exploited by a remote attacker to gain access to sensitive information, modify system configuration or execute code by uploading malicious webservices.

Solution:

Solution type: Mitigation

Change the password.

Vulnerability Insight

It was possible to login with default credentials: admin/axis2

Vulnerability Detection Method

Tries to login with default credentials via HTTP.

Details: `Apache Axis2 Default Credentials (HTTP) - Active Check`

OID:1.3.6.1.4.1.25623.1.0.111006

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2010-0219
url: https://www.exploit-db.com/exploits/15869
url: http://www.securityfocus.com/bid/44055
```

High (CVSS: 10.0)

NVT: Apache Tomcat End of Life (EOL) Detection - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

The Apache Tomcat version on the remote host has reached the end of life (EOL) and should not be used anymore.

Vulnerability Detection Result

```
The "Apache Tomcat" version on the remote host has reached the end of life.
CPE:                   cpe:/a:apache:tomcat:8.0.33
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 8.0.33
Location/URL:      8282/tcp
EOL version:       8.0
EOL date:          2018-06-30
```

Impact

An EOL version of Apache Tomcat is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

Solution type: VendorFix

Update the Apache Tomcat version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if an EOL version is present on the target host.

Details: `Apache Tomcat End of Life (EOL) Detection - Windows`

OID:1.3.6.1.4.1.25623.1.0.108134

Version used: `2024-02-28T14:37:42Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`

Method: `Apache Tomcat Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
url: https://tomcat.apache.org/tomcat-10.0-eol.html
url: https://tomcat.apache.org/tomcat-85-eol.html
url: https://tomcat.apache.org/tomcat-80-eol.html
url: https://tomcat.apache.org/tomcat-70-eol.html
url: https://tomcat.apache.org/tomcat-60-eol.html
url: https://tomcat.apache.org/tomcat-55-eol.html
url: https://en.wikipedia.org/wiki/Apache_Tomcat#Releases
url: https://tomcat.apache.org/whichversion.html
```

High (CVSS: 9.1)

NVT: Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Apache Tomcat is prone to security bypass and information disclosure vulnerabilities.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.37
Installation
path / port:       8282/tcp
```

Impact

Successful exploitation will allow remote attackers to gain access to potentially sensitive information and bypass certain security restrictions.

Solution:

Solution type: VendorFix

Upgrade to Apache Tomcat version 9.0.0.M10 or 8.5.5 or 8.0.37 or 7.0.72 or 6.0.47 or later.

Affected Software/OS

Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, Apache Tomcat versions 8.5.0 to 8.5.4, Apache Tomcat versions 8.0.0.RC1 to 8.0.36, Apache Tomcat versions 7.0.0 to 7.0.70, and Apache Tomcat versions 6.0.0 to 6.0.45 on Windows.

Vulnerability Insight

Multiple flaws exist due to:

- An error in the system property replacement feature for configuration files.
- An error in the realm implementations in Apache Tomcat that does not process the supplied password if the supplied user name did not exist.
- An error in the configured SecurityManager via a Tomcat utility method that is accessible to web applications.
- An error in the configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.
- An error in the ResourceLinkFactory implementation in Apache Tomcat that does not limit web application access to global JNDI resources to those resources explicitly linked to the web application.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Wind.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.811298

Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`

Method: `Apache Tomcat Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.107652)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2016-6794
cve: CVE-2016-0762
cve: CVE-2016-5018
cve: CVE-2016-6796
cve: CVE-2016-6797
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.72
url: http://www.securityfocus.com/bid/93940
url: http://www.securityfocus.com/bid/93944
url: http://www.securityfocus.com/bid/93939
url: http://www.securityfocus.com/bid/93942
url: http://www.securityfocus.com/bid/93943
url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.47
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M10
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.5_and_8
↪.0.37
cert-bund: WID-SEC-2022-1910
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/1031
cert-bund: CB-K17/0659
cert-bund: CB-K17/0397
cert-bund: CB-K17/0133
cert-bund: CB-K16/1927
cert-bund: CB-K16/1673
cert-bund: CB-K16/1646
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-1064
dfn-cert: DFN-CERT-2017-0673
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0137
```

High (CVSS: 9.1)
NVT: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.42
Installation
path / port:       8282/tcp
```

Impact

Successful exploitation will allow remote attackers to obtain sensitive information from requests other then their own.

Solution:

Solution type: VendorFix

Upgrade to version 9.0.0.M18, 8.5.12, 8.0.42, 7.0.76 or later.

Affected Software/OS

Apache Tomcat versions 9.0.0.M1 to 9.0.0.M17,
Apache Tomcat versions 8.5.0 to 8.5.11,
Apache Tomcat versions 8.0.0.RC1 to 8.0.41 and
Apache Tomcat versions 7.0.0 to 7.0.75 on Windows

Vulnerability Insight

A some calls to application listeners did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.810764
Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2017-5648
url: http://tomcat.apache.org/security-9.html
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
url: http://lists.apache.org/thread.html/d0e00f2e147a9e9b13a6829133092f349b2882b
↪f6860397368a52600@%3Cannounce.tomcat.apache.org%3E
cert-bund: WID-SEC-2024-0528
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0047
cert-bund: CB-K17/1257
cert-bund: CB-K17/1246
cert-bund: CB-K17/1060
cert-bund: CB-K17/0801
cert-bund: CB-K17/0604
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-1300
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0624
```

High (CVSS: 7.5)
NVT: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.36
Installation
path / port:       8282/tcp
```

Impact

Successful exploitation will allow remote attackers to cause a denial of service (CPU consumption).

Solution:

Solution type: VendorFix

Upgrade to version 7.0.70, or 8.0.36, or 8.5.3, or 9.0.0.M7, or later.

Affected Software/OS

Apache Tomcat 7.x before 7.0.70, 8.0.0.RC1 before 8.0.36, 8.5.x before 8.5.3, and 9.0.0.M1 before 9.0.0.M7.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The flaw is due to an error in the 'MultipartStream' class in Apache Commons Fileupload when processing multi-part requests.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.808197
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2016-3092
url: http://tomcat.apache.org/security-7.html
url: http://www.securityfocus.com/bid/91453
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-9.html
cert-bund: WID-SEC-2023-0644
cert-bund: WID-SEC-2022-1537
cert-bund: WID-SEC-2022-1375
cert-bund: CB-K18/0605
cert-bund: CB-K17/1750
cert-bund: CB-K17/1198
cert-bund: CB-K17/1060
cert-bund: CB-K17/0657
cert-bund: CB-K17/0397
cert-bund: CB-K16/1993
cert-bund: CB-K16/1799
cert-bund: CB-K16/1758
cert-bund: CB-K16/1322
cert-bund: CB-K16/1002
cert-bund: CB-K16/0993
dfn-cert: DFN-CERT-2023-0574
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0404
```

High (CVSS: 7.5)
NVT: Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.41
Installation
path / port:       8282/tcp
```

Impact

Successful exploitation will allow remote attackers to gain access to potentially sensitive information.

Solution:

Solution type: VendorFix

Upgrade to Apache Tomcat version 9.0.0.M15 or 8.5.9 or 8.0.41 or 7.0.75 or 6.0.50 or later.

Affected Software/OS

Apache Tomcat versions 9.0.0.M1 to 9.0.0.M13, Apache Tomcat versions 8.5.0 to 8.5.8, Apache Tomcat versions 8.0.0.RC1 to 8.0.39, Apache Tomcat versions 7.0.0 to 7.0.73, and Apache Tomcat versions 6.0.16 to 6.0.48 on Windows.

Vulnerability Insight

The flaw exists due to error handling of the send file code for the NIO HTTP connector in Apache Tomcat resulting in the current Processor object being added to the Processor cache multiple times. This in turn means that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.811296

Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`

Method: `Apache Tomcat Detection Consolidation`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2016-8745
url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60409
url: http://www.securityfocus.com/bid/94828
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M15
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9
url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2022-1375
cert-bund: CB-K18/0605
cert-bund: CB-K17/1746
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0801
cert-bund: CB-K17/0444
cert-bund: CB-K17/0397
cert-bund: CB-K17/0303
cert-bund: CB-K17/0133
cert-bund: CB-K17/0090
cert-bund: CB-K16/1929
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2017-1822
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0456
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0308
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2017-0095
```

High (CVSS: 7.5)
NVT: Apache Tomcat DoS Vulnerability (Feb 2023) - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.5.85
Installation
path / port:       8282/tcp
```

Solution:

Solution type: VendorFix

Update to version 8.5.85, 9.0.71, 10.1.5, 11.0.0-M3 or later.

Affected Software/OS

Apache Tomcat versions through 8.5.84, 9.0.0-M1 through 9.0.70, 10.x through 10.1.4 and 11.0.0-M1 only.

Vulnerability Insight

Apache Tomcat uses a packaged renamed copy of Apache Commons FileUpload to provide the file upload functionality defined in the Jakarta Servlet specification. Apache Tomcat was, therefore, also vulnerable to the Apache Commons FileUpload vulnerability CVE-2023-24998 as there was no limit to the number of request parts processed. This resulted in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Tomcat DoS Vulnerability (Feb 2023) - Windows`

OID:1.3.6.1.4.1.25623.1.0.104551

Version used: `2023-10-12T05:05:32Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`

Method: `Apache Tomcat Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2023-24998
url: https://lists.apache.org/thread/g16kv0xpp272htz107molwbbgdrqrdk1
url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3
url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.5
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.71
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.85
url: https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy
cert-bund: WID-SEC-2024-1238
cert-bund: WID-SEC-2024-0890
cert-bund: WID-SEC-2024-0888
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0124
cert-bund: WID-SEC-2024-0117
cert-bund: WID-SEC-2024-0054
cert-bund: WID-SEC-2023-2688
cert-bund: WID-SEC-2023-2675
cert-bund: WID-SEC-2023-2674
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2309
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1817
cert-bund: WID-SEC-2023-1815
cert-bund: WID-SEC-2023-1813
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1811
cert-bund: WID-SEC-2023-1809
cert-bund: WID-SEC-2023-1808
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-1794
cert-bund: WID-SEC-2023-1792
cert-bund: WID-SEC-2023-1791
cert-bund: WID-SEC-2023-1784
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1782
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1142
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-1017
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-1012
cert-bund: WID-SEC-2023-1007
cert-bund: WID-SEC-2023-1005
cert-bund: WID-SEC-2023-0609
cert-bund: WID-SEC-2023-0433
dfn-cert: DFN-CERT-2024-1006
dfn-cert: DFN-CERT-2024-0059
dfn-cert: DFN-CERT-2024-0048
dfn-cert: DFN-CERT-2023-2778
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2469
dfn-cert: DFN-CERT-2023-2054
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1362
dfn-cert: DFN-CERT-2023-1109
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0902
dfn-cert: DFN-CERT-2023-0886
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0763
dfn-cert: DFN-CERT-2023-0574
dfn-cert: DFN-CERT-2023-0540
dfn-cert: DFN-CERT-2023-0414
```

High (CVSS: 7.5)
NVT: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.43
Installation
path / port:       8282/tcp
```

Impact

Successful exploitation will allow remote attackers to obtain sensitive information from requests other then their own.

Solution:

Solution type: VendorFix

Upgrade to version 9.0.0.M19, 8.5.13, 8.0.43, 7.0.77, 6.0.53 or later.

Affected Software/OS

Apache Tomcat versions 9.0.0.M1 to 9.0.0.M18, Apache Tomcat versions 8.5.0 to 8.5.12, Apache Tomcat versions 8.0.0.RC1 to 8.0.42, Apache Tomcat versions 7.0.0 to 7.0.76 and Apache Tomcat versions 6.0.0 to 6.0.52 on Windows.

Vulnerability Insight

A bug in the handling of the pipelined requests when send file was used resulted in the pipelined request being lost when send file processing of the previous request completed.

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability - Windo.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.810762
Version used: `2024-02-15T05:05:40Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2017-5647
url: http://tomcat.apache.org/security-9.html
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
url: http://tomcat.apache.org/security-6.html
url: https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0
↪dee9190ba48171451a@%3Cusers.tomcat.apache.org%3E
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K18/0047
cert-bund: CB-K17/1831
cert-bund: CB-K17/1423
cert-bund: CB-K17/1246
cert-bund: CB-K17/1205
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0801
cert-bund: CB-K17/0604
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-1914
dfn-cert: DFN-CERT-2017-1485
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1243
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0624
```

High (CVSS: 7.5)
NVT: Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
```

... continues on next page ...

. . . continued from previous page . . .

↪7652)

Summary
Apache Tomcat is prone to a security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.53
Installation
path / port:       8282/tcp
```

Impact
Successful exploitation will allow an attacker to bypass certain security restrictions and perform unauthorized actions.

Solution:
Solution type: VendorFix
Upgrade to Apache Tomcat version 9.0.10 or 8.5.32 or 8.0.53 or 7.0.90 or later. Please see the references for more information.

Affected Software/OS
Apache Tomcat versions 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52 and 7.0.35 to 7.0.88 on Windows.

Vulnerability Insight
The flaw exists due to a missing host name verification when using TLS with the WebSocket client.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.813742
Version used: 2024-02-15T05:05:40Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2018-8034
url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C201
↪80722091057.GA70283@minotaur.apache.org%3E
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.53
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.90
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K19/0907
cert-bund: CB-K19/0616
cert-bund: CB-K19/0320
cert-bund: CB-K18/1005
cert-bund: CB-K18/0809
dfn-cert: DFN-CERT-2019-2418
dfn-cert: DFN-CERT-2019-1627
dfn-cert: DFN-CERT-2019-1237
dfn-cert: DFN-CERT-2019-0951
dfn-cert: DFN-CERT-2019-0451
dfn-cert: DFN-CERT-2019-0147
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-1753
dfn-cert: DFN-CERT-2018-1471
dfn-cert: DFN-CERT-2018-1443
dfn-cert: DFN-CERT-2018-1262
```

High (CVSS: 7.5)
NVT: Apache Tomcat Reverse Proxy Information Disclosure Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary
Apache Tomcat is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.39
Installation
path / port:       8282/tcp
```

Impact
Successful exploitation will allow remote attackers to obtain sensitive information from requests other then their own.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Upgrade to version 9.0.0.M17, 8.5.11 or later.

Affected Software/OS

Apache Tomcat versions 9.0.0.M11 to 9.0.0.M15 and Apache Tomcat versions 8.5.0 to 8.5.9 on Windows.

Vulnerability Insight

The refactoring to make wider use of ByteBuffer introduced a regression that could cause information to leak between requests on the same connection. When running behind a reverse proxy, this could result in information leakage between users.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Tomcat Reverse Proxy Information Disclosure Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.810719

Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`

Method: `Apache Tomcat Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2016-8747
url: http://svn.apache.org/viewvc?view=revision&revision=1774161
url: http://www.securityfocus.com/bid/96895
url: http://svn.apache.org/viewvc?view=revision&revision=1774166
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.11
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M17
cert-bund: CB-K17/0426
dfn-cert: DFN-CERT-2017-0433
```

High (CVSS: 7.5)
NVT: Apache Tomcat Security Bypass Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to a security bypass vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.44
Installation
path / port:       8282/tcp
```

Impact

Successful exploitation will allow an attacker to exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:

Solution type: VendorFix

Upgrade to version 9.0.0.M21, or 8.5.15, or 8.0.44, or 7.0.78 or later.

Affected Software/OS

Apache Tomcat 9.0.0.M1 to 9.0.0.M20, Apache Tomcat 8.5.0 to 8.5.14, Apache Tomcat 8.0.0.RC1 to 8.0.43 and Apache Tomcat 7.0.0 to 7.0.77 on Windows

Vulnerability Insight

The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. Tomcat's Default Servlet did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Tomcat Security Bypass Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.811140

Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`

Method: `Apache Tomcat Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2017-5664
url: https://lists.apache.org/thread.html/a42c48e37398d76334e17089e43ccab945238b
↪8b7896538478d76066@%3Cannounce.tomcat.apache.org%3E
url: http://www.securityfocus.com/bid/98888
cert-bund: WID-SEC-2024-0528
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0605
cert-bund: CB-K18/0603
cert-bund: CB-K18/0478
cert-bund: CB-K18/0066
cert-bund: CB-K18/0047
cert-bund: CB-K17/2024
cert-bund: CB-K17/2017
cert-bund: CB-K17/1831
cert-bund: CB-K17/1748
cert-bund: CB-K17/1492
cert-bund: CB-K17/1423
cert-bund: CB-K17/1257
cert-bund: CB-K17/1246
cert-bund: CB-K17/0977
dfn-cert: DFN-CERT-2018-1274
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2018-0513
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-2116
dfn-cert: DFN-CERT-2017-2106
dfn-cert: DFN-CERT-2017-1914
dfn-cert: DFN-CERT-2017-1827
dfn-cert: DFN-CERT-2017-1558
dfn-cert: DFN-CERT-2017-1485
dfn-cert: DFN-CERT-2017-1300
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1011
```

High (CVSS: 7.5)
NVT: Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.52
Installation
path / port:       8282/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow an attacker to conduct a denial-of-service condition.

Solution:
Solution type: VendorFix
Upgrade to Apache Tomcat version 9.0.8 or 8.5.31 or 8.0.52 or 7.0.90 or later. Please see the references for more information.

Affected Software/OS
Apache Tomcat 9.0.0.M9 to 9.0.7 Apache Tomcat 8.5.0 to 8.5.30 Apache Tomcat 8.0.0.RC1 to 8.0.51 Apache Tomcat 7.0.28 to 7.0.86 on Windows.

Vulnerability Insight
The flaw exists due to improper handing of overflow in the UTF-8 decoder with supplementary characters.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813724
Version used: `2024-02-15T05:05:40Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
```
cve: CVE-2018-1336
url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C201
↪80722090435.GA60759%40minotaur.apache.org%3E
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.8
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.31
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.52
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K18/0809
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2018-2474
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-2133
dfn-cert: DFN-CERT-2018-2125
dfn-cert: DFN-CERT-2018-2097
dfn-cert: DFN-CERT-2018-1928
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1753
dfn-cert: DFN-CERT-2018-1541
dfn-cert: DFN-CERT-2018-1471
dfn-cert: DFN-CERT-2018-1443
dfn-cert: DFN-CERT-2018-1262
```

High (CVSS: 7.1)
NVT: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.39
Installation
path / port:       8282/tcp
```

Impact

Successful exploitation will allow remote attackers to poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own.

Solution:

Solution type: VendorFix

Upgrade to version 9.0.0.M13, 8.5.8, 8.0.39, 7.0.73, 6.0.48 or later.

Affected Software/OS

Apache Tomcat versions 9.0.0.M1 to 9.0.0.M11, Apache Tomcat versions 8.5.0 to 8.5.6, Apache Tomcat versions 8.0.0.RC1 to 8.0.38, Apache Tomcat versions 7.0.0 to 7.0.72, and Apache Tomcat versions 6.0.0 to 6.0.47 on Windows.

Vulnerability Insight

The code that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Tomcat HTTP Request Line Information Disclosure Vulnerability - Windows`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.810717
Version used: `2024-02-15T05:05:40Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2016-6816
url: https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48
url: http://www.securityfocus.com/bid/94461
url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13
url: https://qnalist.com/questions/7885204/security-cve-2016-6816-apache-tomcat-
↪information-disclosure
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K17/1746
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0444
cert-bund: CB-K17/0397
cert-bund: CB-K17/0198
cert-bund: CB-K17/0133
cert-bund: CB-K17/0090
cert-bund: CB-K16/1976
cert-bund: CB-K16/1927
cert-bund: CB-K16/1815
dfn-cert: DFN-CERT-2017-1822
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0456
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0203
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-1922
```

[return to 192.168.56.103]

2.1.12 High 445/tcp

High (CVSS: 10.0)
NVT: Microsoft SMB Transaction Parsing Remote Code Execution Vulnerability

Summary
This host is missing a critical security update according to Microsoft Bulletin MS11-020.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to execute arbitrary code on the system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 SP1 and prior
- Microsoft Windows 2008 SP2 and prior
- Microsoft Windows Vista SP2 and prior
- Microsoft Windows 2008 R2 SP1 and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows 2003 Service Pack 2 and prior

Vulnerability Insight
The flaw is due to improper validation of field in SMB request, which allows remote attackers to execute arbitrary code on the system by sending a malformed SMB request.

Vulnerability Detection Method
Details: `Microsoft SMB Transaction Parsing Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902660
Version used: `2022-04-27T12:01:52Z`

References
```
cve: CVE-2011-0661
url: http://www.securitytracker.com/id?1025329
url: http://www.securityfocus.com/bid/47198
url: http://www.us-cert.gov/cas/techalerts/TA11-102A.html
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms
↪11-020
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms
↪11-020
```

High (CVSS: 8.1)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

... continues on next page ...

... continued from previous page ...

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `2023-07-14T16:09:27Z`

References
```
cve: CVE-2017-0143
cve: CVE-2017-0144
cve: CVE-2017-0145
cve: CVE-2017-0146
cve: CVE-2017-0147
cve: CVE-2017-0148
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013078
```

... continues on next page ...

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/96703
url: http://www.securityfocus.com/bid/96704
url: http://www.securityfocus.com/bid/96705
url: http://www.securityfocus.com/bid/96707
url: http://www.securityfocus.com/bid/96709
url: http://www.securityfocus.com/bid/96706
url: https://technet.microsoft.com/library/security/MS17-010
url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448
```

[return to 192.168.56.103]

2.1.13 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Endpoint: ncacn_ip_tcp:192.168.56.103[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49154]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49154]
     Annotation: IKE/Authip API
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49154]
     Annotation: Impl friendly name
Port: 49159/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49159]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
Port: 49180/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.56.103[49180]
Port: 49246/tcp
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49246]
     Annotation: IPSec Policy agent endpoint
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.103[49246]
     Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Solution:

Solution type: Mitigation

Filter incoming traffic to this ports.

Vulnerability Detection Method

Details: DCE/RPC and MSRPC Services Enumeration Reporting

OID:1.3.6.1.4.1.25623.1.0.10736

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2022-06-03T10:17:07Z`

[return to 192.168.56.103]

2.1.14 Medium general/tcp

Medium (CVSS: 6.9)
NVT: Microsoft Windows Kernel Privilege Elevation Vulnerability (3063858)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-063.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to gain elevated privileges on affected system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
The flaw exists in the Windows LoadLibrary as it fails to properly validate user input.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel Privilege Elevation Vulnerability (3063858)`
OID:1.3.6.1.4.1.25623.1.0.805583
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1758
url: https://support.microsoft.com/en-us/kb/3063858
url: http://www.securityfocus.com/bid/75004
url: https://technet.microsoft.com/library/security/MS15-063
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K15/0783
dfn-cert: DFN-CERT-2015-0827
```

Medium (CVSS: 6.9)
NVT: Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Jan 2011)

Summary
A USB device driver software is prone to a code execution vulnerability.

Vulnerability Detection Result

```
File checked for existence: C:\Windows\system32\hidserv.dll
```

Impact
Successful exploitation will allow user-assisted attackers to execute arbitrary programs via crafted USB data.

Solution:
Solution type: Workaround
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
A workaround is to introduce device filtering on the target host to only allow trusted USB devices to be enabled automatically. Once this workaround is in place an overwrite for this vulnerability can be created to mark it as a false positive.

Affected Software/OS
All Microsoft Windows systems with an enabled USB device driver and no local protection mechanism against the automatic enabling of additional Human Interface Device (HID).

Vulnerability Insight
The flaw is due to error in USB device driver (hidserv.dll), which does not properly warn the user before enabling additional Human Interface Device (HID) functionality.

Vulnerability Detection Method
Checks via SMB if a specific device driver (hidserv.dll) exists on the target system.
Details: `Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Ja.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.801581
Version used: `2023-01-12T10:12:15Z`

References

```
cve: CVE-2011-0638
url: http://www.cs.gmu.edu/~astavrou/publications.html
url: http://news.cnet.com/8301-27080_3-20028919-245.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

url: http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou

Medium (CVSS: 6.9)
NVT: Microsoft Windows SCM Privilege_Escalation Vulnerability (3055642)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-050.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow local attacker to gain elevated privileges.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2

Vulnerability Insight
Flaw is due to an error in Service Control Manager (SCM) that is due to a failure to properly verify impersonation levels.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Microsoft Windows SCM Privilege_Escalation Vulnerability (3055642)
OID:1.3.6.1.4.1.25623.1.0.805615
Version used: 2023-07-25T05:05:58Z

References
cve: CVE-2015-1702
url: https://support.microsoft.com/kb/3055642
url: http://www.securityfocus.com/bid/74492
url: https://technet.microsoft.com/library/security/MS15-050
cert-bund: CB-K15/0668
dfn-cert: DFN-CERT-2015-0689

Medium (CVSS: 6.9)
NVT: Microsoft Windows Service Control Manager Privilege Elevation Vulnerability (2872339)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-077.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code with kernel-mode privileges within the context of the Service Control Manager and or corrupt memory.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
The flaw is due to a double-free error in the Service Control Manager (services.exe) when handling service descriptions from the registry.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Service Control Manager Privilege Elevation Vulnerability (28.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902993
Version used: `2022-07-26T10:10:42Z`

References
```
cve: CVE-2013-3862
url: http://support.microsoft.com/kb/2872339
url: http://www.securityfocus.com/bid/62182
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-077
cert-bund: CB-K13/0631
dfn-cert: DFN-CERT-2013-1623
```

Medium (CVSS: 6.9)
NVT: Microsoft Windows Installer Service Privilege Escalation Vulnerability (3072630)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-074.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\msi.dll
File version:     5.0.7601.17514
Vulnerable range: Less than 5.0.7601.18896
```

Impact

Successful exploitation will allow attackers to elevate privileges on a targeted system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight

An elevation of privilege vulnerability exists in some cases in the Windows Installer service when it improperly runs custom action scripts.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Installer Service Privilege Escalation Vulnerability (3072630)`

OID:1.3.6.1.4.1.25623.1.0.805078

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2371
url: https://support.microsoft.com/en-us/kb/3072630
url: https://technet.microsoft.com/en-us/library/security/MS15-074
cert-bund: CB-K15/1037
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1094
dfn-cert: DFN-CERT-2015-1060
```

Medium (CVSS: 6.9)

NVT: Microsoft File Handling Component Remote Code Execution Vulnerability (2922229)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-019.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to execute arbitrary code and potentially compromise user's system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows XP x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight
Flaw is due to an improper path restrictions when processing .bat and .cmd files related to the 'CreateProcess' function.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft File Handling Component Remote Code Execution Vulnerability (2922229)`
OID:1.3.6.1.4.1.25623.1.0.804375
Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-0315
url: http://xforce.iss.net/xforce/xfdb/91356
url: http://www.securityfocus.com/bid/66619
url: https://support.microsoft.com/kb/2922229
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-019
cert-bund: CB-K14/0408
```

Medium (CVSS: 6.8)
NVT: Microsoft USB Mass Storage Class Driver Privilege Elevation Vulnerability (3143142)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-033

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Drivers\Usbstor.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.19144
```

Impact
Successful exploitation will allow an attacker to run arbitrary code in kernel mode.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 10 x32/x64

Vulnerability Insight
The flaw is due to Windows USB Mass Storage Class driver fails to properly validate objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft USB Mass Storage Class Driver Privilege Elevation Vulnerability (3143.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.806898
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0133
url: https://support.microsoft.com/en-us/kb/3139398
url: https://support.microsoft.com/en-us/kb/3124266
url: https://technet.microsoft.com/library/security/MS16-033
cert-bund: CB-K16/0546
cert-bund: CB-K16/0383
```

Medium (CVSS: 6.8)
NVT: Microsoft Windows SAM and LSAD Privilege Elevation Vulnerability (3148527)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-047

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Samsrv.dll
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23390
```

Impact
Successful exploitation will allow an authenticated user to execute code with elevated privileges that could gain access to the SAM database.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 10 x32/x64

Vulnerability Insight
Multiple flaws are due to the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows SAM and LSAD Privilege Elevation Vulnerability (3148527)`
OID:1.3.6.1.4.1.25623.1.0.807660
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0128
url: https://support.microsoft.com/en-us/kb/3148527
url: https://technet.microsoft.com/library/security/MS16-047
cert-bund: CB-K16/0546
```

Medium (CVSS: 6.8)
NVT: Oracle Java SE Security Update (oct2021) 02 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability and confidentiality.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u301 (1.8.0.301) and earlier, 11.0.12 and earlier, 17 and earlier on Windows.

Vulnerability Insight
Multiple flaws are due to multiple errors in 'Libraries' and 'JSSE' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2021) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818828
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-35567
cve: CVE-2021-35578
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
cert-bund: WID-SEC-2023-0426
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0908
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0196
cert-bund: CB-K22/0310
cert-bund: CB-K22/0239
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K21/1082
dfn-cert: DFN-CERT-2022-1721
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-0580
dfn-cert: DFN-CERT-2022-0366
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2021-2566
```

Medium (CVSS: 6.8)
NVT: Oracle Java SE Security Update (oct2021) 02 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability and confidentiality.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u301 (1.8.0.301) and earlier, 11.0.12 and earlier, 17 and earlier on Windows.

Vulnerability Insight
Multiple flaws are due to multiple errors in 'Libraries' and 'JSSE' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2021) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818828
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-35567
cve: CVE-2021-35578
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-0426
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0908
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0196
cert-bund: CB-K22/0310
cert-bund: CB-K22/0239
cert-bund: CB-K21/1082
dfn-cert: DFN-CERT-2022-1721
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-0580
dfn-cert: DFN-CERT-2022-0366
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2021-2566
```

Medium (CVSS: 6.1)
NVT: Microsoft Windows Network Location Awareness Service Security Bypass Vulnerability (3022777)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-005.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to relax the firewall policy and/or configuration of certain services by spoofing responses of DNS or LDAP traffic via a Man-in-the-Middle attack.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight

The flaw is due to an error within the Network Location Awareness (NLA) service when validating if a domain-connected computer is connected to the domain.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Network Location Awareness Service Security Bypass Vulnerabil.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.805036

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0006
url: https://support.microsoft.com/en-us/topic/ms15-005-vulnerability-in-network
↪-location-awareness-service-could-allow-security-feature-bypass-january-13-201
↪5-5a2f60a5-f721-4e2c-2a52-c4a8dd4c3b95
url: http://www.securityfocus.com/bid/71930
url: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms
↪15-005
cert-bund: CB-K15/0038
dfn-cert: DFN-CERT-2015-0036
```

Medium (CVSS: 6.1)
NVT: Microsoft Windows IIS Privilege Escalation Vulnerability (4013074)

Summary

This host is missing an important security update according to Microsoft Bulletin MS17-016

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23677
```

Impact

Successful exploitation will allow an attacker to perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on behalf of the victim, and inject malicious content in the victim's browser.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2016

Vulnerability Insight

The flaw exists due to Microsoft IIS Server fails to properly sanitize a specially crafted request.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows IIS Privilege Escalation Vulnerability (4013074)`

OID:1.3.6.1.4.1.25623.1.0.810815

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2017-0055
url: https://support.microsoft.com/en-us/kb/4013074
url: http://www.securityfocus.com/bid/96622
url: https://technet.microsoft.com/en-us/library/security/MS17-016
url: https://technet.microsoft.com/library/security/MS17-016
cert-bund: CB-K17/0440
dfn-cert: DFN-CERT-2017-0447
```

Medium (CVSS: 5.9)

NVT: Oracle Java SE Security Update (jan2024) 03 - Windows

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to compromise Oracle Java SE, which can result in unauthorized access to critical data or complete access to all Oracle Java SE.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u391 and earlier 11.0.21 and earlier on Windows.

Vulnerability Insight
The flaw exists due to an unspecified vulnerability in Oracle Java SE which can be exploited by using APIs in the specified Component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2024) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832789
Version used: `2024-01-24T05:06:24Z`

References
```
cve: CVE-2024-20926
url: https://www.oracle.com/security-alerts/cpujan2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0121
dfn-cert: DFN-CERT-2024-0500
dfn-cert: DFN-CERT-2024-0494
dfn-cert: DFN-CERT-2024-0422
dfn-cert: DFN-CERT-2024-0361
dfn-cert: DFN-CERT-2024-0354
dfn-cert: DFN-CERT-2024-0129
dfn-cert: DFN-CERT-2024-0128
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Update (jul2023) 02 - Windows

Summary
Oracle Java SE is prone to remote code execution (RCE) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u371 and earlier on Windows.

Vulnerability Insight
The flaw is due to improper application of networking protocols within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jul2023) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832160
Version used: `2023-10-13T05:06:10Z`

References
```
cve: CVE-2023-22043
url: https://www.oracle.com/security-alerts/cpujul2023.html
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2681
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1653
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Update (oct2021) 03 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability and confidentiality.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u301 (1.8.0.301) and earlier, 7u311 (1.7.0.311) and earlier, 11.0.12 and earlier on Windows.

Vulnerability Insight

Multiple flaws are due to multiple errors in 'JSSE' component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2021) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818829
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-35550
cve: CVE-2021-35565
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0908
cert-bund: WID-SEC-2022-0871
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0674
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0484
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0386
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0196
cert-bund: WID-SEC-2022-0024
cert-bund: CB-K22/0675
cert-bund: CB-K22/0239
cert-bund: CB-K21/1082
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2022-1721
dfn-cert: DFN-CERT-2022-1571
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1456
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1247
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Update (jul2023) 02 - Windows

Summary
Oracle Java SE is prone to remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u371 and earlier on Windows.

Vulnerability Insight
The flaw is due to improper application of networking protocols within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jul2023) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832160
Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-22043
url: https://www.oracle.com/security-alerts/cpujul2023.html
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2681
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1653
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Update (oct2021) 03 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability and confidentiality.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u301 (1.8.0.301) and earlier, 7u311 (1.7.0.311) and earlier, 11.0.12 and earlier on Windows.

Vulnerability Insight
Multiple flaws are due to multiple errors in 'JSSE' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2021) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818829
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-35550
cve: CVE-2021-35565
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0908
cert-bund: WID-SEC-2022-0871
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0674
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0484
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0386
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0196
cert-bund: WID-SEC-2022-0024
cert-bund: CB-K22/0675
cert-bund: CB-K22/0239
cert-bund: CB-K21/1082
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2022-1721
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1456
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1247
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Update (apr2021) - Windows

Summary
Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on integrity.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 7u291 (1.7.0.291) and earlier, 8u281 (1.8.0.281) and earlier, 11.0.10 and earlier, 16 on Windows.

Vulnerability Insight
Multiple flaws are due to multiple errors in 'Libraries' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (apr2021) - Windows`
OID:1.3.6.1.4.1.25623.1.0.818127
Version used: `2023-04-03T10:19:50Z`

References
```
cve: CVE-2021-2161
cve: CVE-2021-2163
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixJAVA
cert-bund: WID-SEC-2023-1125
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1303
cert-bund: WID-SEC-2022-1261
cert-bund: WID-SEC-2022-1244
cert-bund: CB-K21/0981
cert-bund: CB-K21/0412
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2022-1934
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Update (apr2023) 02 - Windows

Summary
Oracle Java SE is prone to a remote code execution vulnerability.

Vulnerability Detection Result
```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u361 and earlier, 11.0.18, 17.0.6 and earlier on Windows.

Vulnerability Insight

The flaw is due to improper application of networking protocols within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (apr2023) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832048

Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-21954
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2112
cert-bund: WID-SEC-2023-1011
dfn-cert: DFN-CERT-2023-2493
dfn-cert: DFN-CERT-2023-2249
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1879
dfn-cert: DFN-CERT-2023-1418
dfn-cert: DFN-CERT-2023-1336
dfn-cert: DFN-CERT-2023-0897
dfn-cert: DFN-CERT-2023-0896
```

Medium (CVSS: 5.9)

NVT: Oracle Java SE Security Update (apr2021) - Windows

Summary

Oracle Java SE is prone to multiple security vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to have an impact on integrity.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 7u291 (1.7.0.291) and earlier, 8u281 (1.8.0.281) and earlier, 11.0.10 and earlier, 16 on Windows.

Vulnerability Insight

Multiple flaws are due to multiple errors in 'Libraries' component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (apr2021) - Windows`

OID:1.3.6.1.4.1.25623.1.0.818127

Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-2161
cve: CVE-2021-2163
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixJAVA
cert-bund: WID-SEC-2023-1125
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1303
cert-bund: WID-SEC-2022-1261
cert-bund: WID-SEC-2022-1244
cert-bund: CB-K21/0981
cert-bund: CB-K21/0412
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2022-1934
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Update (jan2024) 03 - Windows

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to compromise Oracle Java SE, which can result in unauthorized access to critical data or complete access to all Oracle Java SE.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u391 and earlier 11.0.21 and earlier on Windows.

Vulnerability Insight
The flaw exists due to an unspecified vulnerability in Oracle Java SE which can be exploited by using APIs in the specified Component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2024) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832789
Version used: `2024-01-24T05:06:24Z`

References

```
cve: CVE-2024-20926
url: https://www.oracle.com/security-alerts/cpujan2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0121
dfn-cert: DFN-CERT-2024-0500
dfn-cert: DFN-CERT-2024-0494
dfn-cert: DFN-CERT-2024-0422
dfn-cert: DFN-CERT-2024-0361
dfn-cert: DFN-CERT-2024-0354
dfn-cert: DFN-CERT-2024-0129
dfn-cert: DFN-CERT-2024-0128
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Update (apr2023) 02 - Windows

Summary
Oracle Java SE is prone to a remote code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u361 and earlier, 11.0.18, 17.0.6 and earlier on Windows.

Vulnerability Insight
The flaw is due to improper application of networking protocols within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (apr2023) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832048
Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-21954
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2112
cert-bund: WID-SEC-2023-1011
dfn-cert: DFN-CERT-2023-2493
dfn-cert: DFN-CERT-2023-2249
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1879
dfn-cert: DFN-CERT-2023-1418
dfn-cert: DFN-CERT-2023-1336
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0897
dfn-cert: DFN-CERT-2023-0896
```

Medium (CVSS: 5.8)
NVT: Microsoft Root Certificate Program SHA-1 Deprecation Advisory (3123479)

Summary
This host is missing an important security update according to Microsoft advisory (3123479).

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23584
```

Impact
Successful exploitation will allow attackers to take advantage of weakness of the SHA-1 hashing algorithm that exposes it to collision attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1

Vulnerability Insight
An update is available that aims to warn customers in assessing the risk of certain applications that use X.509 digital certificates that are signed using the SHA-1 hashing algorithm.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Root Certificate Program SHA-1 Deprecation Advisory (3123479)`
OID:1.3.6.1.4.1.25623.1.0.806663
Version used: `2023-07-21T05:05:22Z`

References

```
url: https://support.microsoft.com/en-us/help/3197869
url: https://support.microsoft.com/en-us/help/3197875
url: https://support.microsoft.com/en-us/help/3198585
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://support.microsoft.com/en-us/help/3198586
url: https://support.microsoft.com/en-us/help/3200970
url: https://support.microsoft.com/en-us/kb/3123479
url: https://technet.microsoft.com/en-us/library/security/3123479
url: http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-en
↪forcement-of-authenticode-code-signing-and-timestamping.aspx
```

Medium (CVSS: 5.8)
NVT: Microsoft Windows IP-HTTPS Component Security Feature Bypass Vulnerability (2765809)

Summary
This host is missing an important security update according to Microsoft Bulletin MS12-083.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow attacker to bypass certain security restrictions.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior.

Vulnerability Insight
The flaw is due to error in the IP-HTTPS component, which fails to validate the certificates. This can lead to a revoked certificate being considered as valid.

Vulnerability Detection Method
Details: `Microsoft Windows IP-HTTPS Component Security Feature Bypass Vulnerability (276.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.901305
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2012-2549
url: http://support.microsoft.com/kb/2765809
url: http://www.securityfocus.com/bid/56840
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-083
dfn-cert: DFN-CERT-2012-2231
```

Medium (CVSS: 5.8)
NVT: Microsoft Schannel Security Bypass Vulnerability (3081320)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-121.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\schannel.dll
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.19044
```

Impact
Successful exploitation will allow attackers to perform unauthorized actions by conducting a man-in-the-middle attack and this may lead to other attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
The flaw is due to some weakness in the Transport Layer Security (TLS) implementation.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Schannel Security Bypass Vulnerability (3081320)`
OID:1.3.6.1.4.1.25623.1.0.806555
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-6112
url: https://support.microsoft.com/en-us/kb/3081320
url: https://technet.microsoft.com/library/security/MS15-121
cert-bund: CB-K15/1649
dfn-cert: DFN-CERT-2015-1742
```

Medium (CVSS: 5.5)
NVT: Microsoft Graphics Component 'gdi32.dll' Information Disclosure Vulnerability (MS17-013)

Summary
'gdi32.dll' Graphics Device Interface is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Gdi32.dll
File version:     6.1.7601.17514
Vulnerable range: Version 6.1.7601.23457 and prior
```

Impact
Successful exploitation will allow an attacker to obtain sensitive information from process heap memory.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511, 1607 x32/x64
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1

Vulnerability Insight
The flaw exists due to multiple bugs related to the handling of DIBs (Device Independent Bitmaps) embedded in EMF records.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Graphics Component 'gdi32.dll' Information Disclosure Vulnerability (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809889
Version used: `2023-06-23T16:09:17Z`

References

```
cve: CVE-2017-0038
url: https://bugs.chromium.org/p/project-zero/issues/detail?id=992
url: https://technet.microsoft.com/library/security/MS17-013
cert-bund: CB-K17/0443
dfn-cert: DFN-CERT-2017-0451
```

Medium (CVSS: 5.5)
NVT: Microsoft Windows Registry Multiple Vulnerabilities (3193227)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-124

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\
toskrnl.exe
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.23564
```

Impact
Successful exploitation will allow attacker to gain access to information not intended to be available to the user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64

Vulnerability Insight
Multiple elevation of privilege vulnerabilities exist in Microsoft Windows when a Windows kernel API improperly allows a user to access sensitive registry information.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Registry Multiple Vulnerabilities (3193227)`
OID:1.3.6.1.4.1.25623.1.0.809440
Version used: `2023-09-22T16:08:59Z`

References

```
cve: CVE-2016-0070
cve: CVE-2016-0073
cve: CVE-2016-0075
cve: CVE-2016-0079
url: https://support.microsoft.com/en-us/kb/3193227
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/93354
url: http://www.securityfocus.com/bid/93355
url: http://www.securityfocus.com/bid/93356
url: http://www.securityfocus.com/bid/93357
url: https://technet.microsoft.com/en-us/library/security/MS16-124
url: https://technet.microsoft.com/library/security/MS16-124
cert-bund: CB-K16/1582
```

Medium (CVSS: 5.5)
NVT: Microsoft Windows Common Log File System Driver Information Disclosure Vulnerability (3207328)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-153.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\clfs.sys
File version:     6.1.7600.16385
Vulnerable range: Less than 6.1.7601.23598
```

Impact
Successful exploitation will allow an attacker to run a specially crafted application to bypass security measures on the affected system allowing further exploitation.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2016 x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64

Vulnerability Insight
The flaw exists due to the Windows Common Log File System (CLFS) driver improperly handles objects in memory.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Common Log File System Driver Information Disclosure Vulnerab.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.810310
Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-7295
url: https://support.microsoft.com/en-us/kb/3207328
url: http://www.securityfocus.com/bid/94787
url: https://technet.microsoft.com/en-us/library/security/MS16-153
url: https://technet.microsoft.com/library/security/MS16-0153
cert-bund: CB-K16/1959
```

Medium (CVSS: 5.5)
NVT: Microsoft Windows Kernel Elevation of Privilege Vulnerability (3199720)

Summary

This host is missing an important security update according to Microsoft Bulletin MS16-139.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Ntoskrnl.exe
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.23569
```

Impact

Successful exploitation will allow an attacker could gain access to information that is not intended for the user.

Solution:

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1

Vulnerability Insight

The flaw exists in the way that the Windows Kernel API enforces permissions.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kernel Elevation of Privilege Vulnerability (3199720)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.809467
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-7216
url: https://support.microsoft.com/en-us/kb/3199720
url: http://www.securityfocus.com/bid/94048
url: https://technet.microsoft.com/library/security/MS16-139
url: https://technet.microsoft.com/en-us/library/security/MS16-139
cert-bund: CB-K16/1747
```

Medium (CVSS: 5.4)
NVT: Microsoft Windows SAMR Protocol Security Bypass Vulnerability (2934418)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-016.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to bypass certain security features.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Vulnerability Insight
Flaw is due to improper validation of user lockout state by Security Account Manager Remote (SAMR) protocol .

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows SAMR Protocol Security Bypass Vulnerability (2934418)`
OID:1.3.6.1.4.1.25623.1.0.804245

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2014-0317
url: http://support.microsoft.com/kb/2934418
url: http://www.securityfocus.com/bid/66012
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-016
cert-bund: CB-K14/0296
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (jan2022) 04 - Windows

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to have an impact on availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u311 (1.8.0.311) and earlier, 7u321 (1.7.0.321) and earlier and 11.x through 11.0.13 on Windows.

Vulnerability Insight

The flaw is due to an error in 'Libraries' component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jan2022) 04 - Windows`

OID:1.3.6.1.4.1.25623.1.0.819967

Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2022-21271
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixJAVA
cert-bund: WID-SEC-2022-0432
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0100
cert-bund: CB-K22/0078
cert-bund: CB-K22/0061
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0111
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (jan2022) 01 - Windows

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u311 (1.8.0.311) and earlier, 7u321 (1.7.0.321) and earlier on Windows.

Vulnerability Insight
The flaw is due to an error in ’2D’ component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2022) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.819964
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2022-21349
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixJAVA
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0839
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0812
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0431
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0100
cert-bund: CB-K22/0078
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0111
```

Medium (CVSS: 5.3)
NVT: Microsoft Windows NPS RADIUS Server Denial of Service Vulnerability (3133043)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-021

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Iassam.dll
File version:     6.1.7600.16385
Vulnerable range: Less than 6.1.7601.19114
```

Impact
Successful exploitation will allow a remote attacker to send specially crafted username strings to a Network Policy Server (NPS) causing a denial of service condition for RADIUS authentication on the NPS.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2012/2012R2

Vulnerability Insight
The flaw is due to an improper handling of a Remote Authentication Dial-In User Service (RADIUS) authentication request in Network Policy Server (NPS).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Microsoft Windows NPS RADIUS Server Denial of Service Vulnerability (3133043)`
OID:1.3.6.1.4.1.25623.1.0.806864
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2016-0050
url: https://support.microsoft.com/en-us/kb/3133043
url: https://technet.microsoft.com/library/security/MS16-021
cert-bund: CB-K16/0220
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2021) 04 - Windows

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to have an impact on availability and confidentiality.

Solution:

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u301 (1.8.0.301) and earlier, 7u311 (1.7.0.311) and earlier, 11.0.12 and earlier and 17.0.0.

Vulnerability Insight

Multiple flaws are due to multiple errors in the 'ImageIO', 'Keytool', 'Swing', 'Utility' and 'JSSE' components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2021) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818830
Version used: `2023-04-03T10:19:50Z`

References

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2021-35586
cve: CVE-2021-35564
cve: CVE-2021-35556
cve: CVE-2021-35559
cve: CVE-2021-35561
cve: CVE-2021-35603
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-1162
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0908
cert-bund: WID-SEC-2022-0871
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0674
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0398
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0196
cert-bund: WID-SEC-2022-0028
cert-bund: WID-SEC-2022-0024
cert-bund: CB-K22/0675
cert-bund: CB-K22/0239
cert-bund: CB-K21/1082
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2022-1721
dfn-cert: DFN-CERT-2022-1704
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1456
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1247
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
dfn-cert: DFN-CERT-2021-2566
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2021) 04 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability and confidentiality.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u301 (1.8.0.301) and earlier, 7u311 (1.7.0.311) and earlier, 11.0.12 and earlier and 17.0.0.

Vulnerability Insight
Multiple flaws are due to multiple errors in the 'ImageIO', 'Keytool', 'Swing', 'Utility' and 'JSSE' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2021) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818830
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-35586
cve: CVE-2021-35564
cve: CVE-2021-35556
cve: CVE-2021-35559
cve: CVE-2021-35561
cve: CVE-2021-35603
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-1162
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0908
cert-bund: WID-SEC-2022-0871
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0674
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0398
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0196
cert-bund: WID-SEC-2022-0028
cert-bund: WID-SEC-2022-0024
cert-bund: CB-K22/0675
cert-bund: CB-K22/0239
cert-bund: CB-K21/1082
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2022-1721
dfn-cert: DFN-CERT-2022-1704
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1456
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1247
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
dfn-cert: DFN-CERT-2021-2566
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2022) 04 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attacker to have an impact on availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u341 and earlier, 11.x through 11.0.16.1 on Windows.

Vulnerability Insight

The flaw exists due to an error in component 'Security'.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (oct2022) 04 - Windows`

OID:1.3.6.1.4.1.25623.1.0.826593

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-21626
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0809
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1789
dfn-cert: DFN-CERT-2023-0616
dfn-cert: DFN-CERT-2023-0608
dfn-cert: DFN-CERT-2023-0607
dfn-cert: DFN-CERT-2023-0217
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2696
dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2600
dfn-cert: DFN-CERT-2022-2547
dfn-cert: DFN-CERT-2022-2313
dfn-cert: DFN-CERT-2022-2312
```

Medium (CVSS: 5.3)

NVT: Microsoft Active Directory Federation Services Information Disclosure Vulnerability (4010320)

Summary

This host is missing an important security update according to Microsoft Bulletin MS17-019.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
File checked:     C:\Windows\System32\Win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23677
```

Impact

Successful exploitation will allow an attacker to read sensitive information about the target system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2012/2012R2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2016

Vulnerability Insight

The flaw exists when Windows Active Directory Federation Services (ADFS) honors XML External Entities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Active Directory Federation Services Information Disclosure Vulnerabi.`
↪..

OID:1.3.6.1.4.1.25623.1.0.810813

Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0043
url: https://support.microsoft.com/en-us/kb/4010320
url: http://www.securityfocus.com/bid/96628
url: https://technet.microsoft.com/library/security/MS17-019
url: https://technet.microsoft.com/library/security/MS17-019
cert-bund: CB-K17/0443
dfn-cert: DFN-CERT-2017-0451
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (jan2023) 02 - Windows

Summary

Oracle Java SE is prone to an input validation vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to manipulate data.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u351 and earlier on Windows.

Vulnerability Insight

The flaw is due to an improper input validation within the Serialization component in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jan2023) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.826785

Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-21830
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-1813
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0840
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0128
dfn-cert: DFN-CERT-2023-1425
dfn-cert: DFN-CERT-2023-1174
dfn-cert: DFN-CERT-2023-1139
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0717
dfn-cert: DFN-CERT-2023-0605
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0125
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0124
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2022) 01 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u341 and earlier, 11.x through 11.0.16.1, 17.x through 17.0.4.1, 19 on Windows.

Vulnerability Insight
Multiple flaws exist due to multiple errors in components 'JNDI', 'Security' and 'JNDI'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2022) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.826589
Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-21628
cve: CVE-2022-21619
cve: CVE-2022-21624
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0809
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1789
dfn-cert: DFN-CERT-2023-0616
dfn-cert: DFN-CERT-2023-0256
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0217
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2696
dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2600
dfn-cert: DFN-CERT-2022-2547
dfn-cert: DFN-CERT-2022-2313
dfn-cert: DFN-CERT-2022-2312
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (jan2023) 02 - Windows

Summary
Oracle Java SE is prone to an input validation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to manipulate data.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u351 and earlier on Windows.

Vulnerability Insight
The flaw is due to an improper input validation within the Serialization component in Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2023) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.826785
Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-21830
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-1813
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0840
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0128
dfn-cert: DFN-CERT-2023-1425
dfn-cert: DFN-CERT-2023-1174
dfn-cert: DFN-CERT-2023-1139
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0717
dfn-cert: DFN-CERT-2023-0605
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0125
dfn-cert: DFN-CERT-2023-0124
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2022) 04 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u341 and earlier, 11.x through 11.0.16.1 on Windows.

Vulnerability Insight
The flaw exists due to an error in component 'Security'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Oracle Java SE Security Update (oct2022) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.826593
Version used: 2023-10-19T05:05:21Z

References

```
cve: CVE-2022-21626
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0809
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1789
dfn-cert: DFN-CERT-2023-0616
dfn-cert: DFN-CERT-2023-0608
dfn-cert: DFN-CERT-2023-0607
dfn-cert: DFN-CERT-2023-0217
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2696
dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2600
dfn-cert: DFN-CERT-2022-2547
dfn-cert: DFN-CERT-2022-2313
dfn-cert: DFN-CERT-2022-2312
```

Medium (CVSS: 5.3)
NVT: Microsoft Internet Messaging API Information Disclosure Vulnerability (3196067)

Summary
This host is missing a moderate security update according to Microsoft Bulletin MS16-126.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\win32k.sys
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.23545
```

Impact
Successful exploitation will allow an attacker to test for the presence of files on disk.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64

Vulnerability Insight
An information disclosure vulnerability exists when the Microsoft Internet Messaging API improperly handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Internet Messaging API Information Disclosure Vulnerability (3196067)`
OID:1.3.6.1.4.1.25623.1.0.809345
Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-3298
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/3196067
url: http://www.securityfocus.com/bid/93392
url: https://technet.microsoft.com/library/security/MS16-126
url: https://technet.microsoft.com/en-us/library/security/MS16-126
cert-bund: CB-K16/1582
cert-bund: CB-K16/1572
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (jan2022) 04 - Windows

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle Java SE version 8u311 (1.8.0.311) and earlier, 7u321 (1.7.0.321) and earlier and 11.x through 11.0.13 on Windows.

Vulnerability Insight
The flaw is due to an error in 'Libraries' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2022) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.819967
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2022-21271
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixJAVA
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0100
cert-bund: CB-K22/0078
cert-bund: CB-K22/0061
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0111
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (jan2022) 02 - Windows

Summary
Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     See vendor advisory
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability, integrity and confidentiality.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u311 (1.8.0.311) and earlier, 7u321 (1.7.0.321) and earlier, 11.x through 11.0.13 and 17.x through 17.0.1 on Windows.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors in components 'Serialization', 'Libraries', 'JAXP', 'ImageIO' and 'Hotspot'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2022) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.819965
Version used: `2023-10-19T05:05:21Z`

References
```
cve: CVE-2022-21291
cve: CVE-2022-21305
cve: CVE-2022-21360
cve: CVE-2022-21365
cve: CVE-2022-21282
cve: CVE-2022-21296
cve: CVE-2022-21299
cve: CVE-2022-21293
cve: CVE-2022-21294
cve: CVE-2022-21340
cve: CVE-2022-21341
cve: CVE-2022-21248
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixJAVA
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0812
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0446
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0431
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0287
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0100
cert-bund: WID-SEC-2022-0028
cert-bund: CB-K22/0078
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1323
dfn-cert: DFN-CERT-2022-1266
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0111
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (jan2022) 02 - Windows

Summary
Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     See vendor advisory
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability, integrity and confidentiality.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u311 (1.8.0.311) and earlier, 7u321 (1.7.0.321) and earlier, 11.x through 11.0.13 and 17.x through 17.0.1 on Windows.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors in components ’Serialization’, ’Libraries’, ’JAXP’, ’ImageIO’ and ’Hotspot’.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jan2022) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.819965

Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-21291
cve: CVE-2022-21305
cve: CVE-2022-21360
cve: CVE-2022-21365
cve: CVE-2022-21282
cve: CVE-2022-21296
cve: CVE-2022-21299
cve: CVE-2022-21293
cve: CVE-2022-21294
cve: CVE-2022-21340
cve: CVE-2022-21341
cve: CVE-2022-21248
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixJAVA
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0812
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0431
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0287
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0100
cert-bund: WID-SEC-2022-0028
cert-bund: CB-K22/0078
dfn-cert: DFN-CERT-2022-1648
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1323
dfn-cert: DFN-CERT-2022-1266
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0111
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (jan2022) 01 - Windows

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u311 (1.8.0.311) and earlier, 7u321 (1.7.0.321) and earlier on Windows.

Vulnerability Insight
The flaw is due to an error in '2D' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2022) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.819964
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2022-21349
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixJAVA
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2023-0838
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0812
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0431
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0100
cert-bund: CB-K22/0078
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0111
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2022) 01 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u341 and earlier, 11.x through 11.0.16.1, 17.x through 17.0.4.1, 19 on Windows.

Vulnerability Insight
Multiple flaws exist due to multiple errors in components 'JNDI', 'Security' and 'JNDI'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2022) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.826589
Version used: `2023-10-19T05:05:21Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2022-21628
cve: CVE-2022-21619
cve: CVE-2022-21624
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0809
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1789
dfn-cert: DFN-CERT-2023-0616
dfn-cert: DFN-CERT-2023-0256
dfn-cert: DFN-CERT-2023-0217
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2696
dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2600
dfn-cert: DFN-CERT-2022-2547
dfn-cert: DFN-CERT-2022-2313
dfn-cert: DFN-CERT-2022-2312
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2023) 03 - Windows

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to compromise Oracle Java SE, which can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u381, 11.0.20, 17.0.8, 20.0.2 on Windows.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The flaw exists due to an unspecified vulnerability in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2023) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832605
Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2023-22081
url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2024-0521
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2692
dfn-cert: DFN-CERT-2024-0169
dfn-cert: DFN-CERT-2023-3177
dfn-cert: DFN-CERT-2023-3009
dfn-cert: DFN-CERT-2023-3006
dfn-cert: DFN-CERT-2023-2999
dfn-cert: DFN-CERT-2023-2975
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2023-2886
dfn-cert: DFN-CERT-2023-2562
dfn-cert: DFN-CERT-2023-2561
dfn-cert: DFN-CERT-2023-2560
dfn-cert: DFN-CERT-2023-2559
dfn-cert: DFN-CERT-2023-2558
dfn-cert: DFN-CERT-2023-2557
dfn-cert: DFN-CERT-2023-2535
dfn-cert: DFN-CERT-2023-2534
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2023) 03 - Windows

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attacker to compromise Oracle Java SE, which can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u381, 11.0.20, 17.0.8, 20.0.2 on Windows.

Vulnerability Insight

The flaw exists due to an unspecified vulnerability in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (oct2023) 03 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832605

Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2023-22081
url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2024-0521
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2692
dfn-cert: DFN-CERT-2024-0169
dfn-cert: DFN-CERT-2023-3177
dfn-cert: DFN-CERT-2023-3009
dfn-cert: DFN-CERT-2023-3006
dfn-cert: DFN-CERT-2023-2999
dfn-cert: DFN-CERT-2023-2975
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2023-2886
dfn-cert: DFN-CERT-2023-2562
dfn-cert: DFN-CERT-2023-2561
dfn-cert: DFN-CERT-2023-2560
dfn-cert: DFN-CERT-2023-2559
dfn-cert: DFN-CERT-2023-2558
dfn-cert: DFN-CERT-2023-2557
dfn-cert: DFN-CERT-2023-2535
dfn-cert: DFN-CERT-2023-2534
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2023) 01 - Windows

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to compromise Oracle Java SE. It can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u381 and earlier, on Windows.

Vulnerability Insight
The flaw exists due to an unspecified vulnerability in Oracle Java SE which can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2023) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832602
Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2023-22067
url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2692
dfn-cert: DFN-CERT-2023-3177
dfn-cert: DFN-CERT-2023-3009
dfn-cert: DFN-CERT-2023-3006
dfn-cert: DFN-CERT-2023-2999
dfn-cert: DFN-CERT-2023-2975
dfn-cert: DFN-CERT-2023-2941
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2023-2886
dfn-cert: DFN-CERT-2023-2562
dfn-cert: DFN-CERT-2023-2557
dfn-cert: DFN-CERT-2023-2534
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Update (oct2023) 01 - Windows

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to compromise Oracle Java SE. It can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u381 and earlier, on Windows.

Vulnerability Insight
The flaw exists due to an unspecified vulnerability in Oracle Java SE which can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2023) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832602
Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2023-22067
url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0528
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2692
dfn-cert: DFN-CERT-2023-3177
dfn-cert: DFN-CERT-2023-3009
dfn-cert: DFN-CERT-2023-3006
dfn-cert: DFN-CERT-2023-2999
dfn-cert: DFN-CERT-2023-2975
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2023-2886
dfn-cert: DFN-CERT-2023-2562
dfn-cert: DFN-CERT-2023-2557
dfn-cert: DFN-CERT-2023-2534
```

Medium (CVSS: 5.1)
NVT: Oracle Java SE Security Update (jul2023) 03 - Windows

Summary
Oracle Java SE is prone to remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u371 and earlier, 11.0.19, 17.0.7, 20.0.1 and earlier on Windows.

Vulnerability Insight
The flaw is due to improper application of hotspot module within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jul2023) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832318
Version used: `2023-10-13T05:06:10Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2023-22041
url: https://www.oracle.com/security-alerts/cpujul2023.html
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1814
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1972
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1657
dfn-cert: DFN-CERT-2023-1653
```

Medium (CVSS: 5.1)
NVT: Oracle Java SE Security Update (jul2023) 03 - Windows

Summary
Oracle Java SE is prone to remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u371 and earlier, 11.0.19, 17.0.7, 20.0.1 and earlier on Windows.

Vulnerability Insight
The flaw is due to improper application of hotspot module within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jul2023) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832318
Version used: `2023-10-13T05:06:10Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2023-22041
url: https://www.oracle.com/security-alerts/cpujul2023.html
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1814
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1972
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1657
dfn-cert: DFN-CERT-2023-1653
```

Medium (CVSS: 5.0)
NVT: Microsoft Internet Explorer PDF Information Disclosure Vulnerability (Nov 2009)

Summary
Internet Explorer is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful attacks which may leads to the exposure of system information on the affected system.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
Microsoft Internet Explorer version 6/7/8.

Vulnerability Insight
The weakness is due to an Internet Explorer including the first 63 bytes of the file path in the 'Title' property when converting local HTML or MHT files to PDF using a PDF printer. This can lead to the exposure of certain system information e.g. the user name.

Vulnerability Detection Method
Details: `Microsoft Internet Explorer PDF Information Disclosure Vulnerability (Nov 2009)`
OID:1.3.6.1.4.1.25623.1.0.900897
Version used: `2024-02-19T05:05:57Z`

References

```
cve: CVE-2009-4073
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/archive/1/archive/1/508010/100/0/threaded
url: http://www.securityfocus.com/bid/37117
url: http://www.theregister.co.uk/2009/11/23/internet_explorer_file_disclosure_b
↪ug/
url: http://securethoughts.com/2009/11/millions-of-pdf-invisibly-embedded-with-y
↪our-internal-disk-paths/
```

Medium (CVSS: 5.0)
NVT: Microsoft Schannel Information Disclosure Vulnerability (3061518)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-055.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow remote attacker to gain access to potentially sensitive information.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 2003 x32/x64 Service Pack 2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2

Vulnerability Insight
The flaw is due to the use of a weak Diffie-Hellman ephemeral (DFE) key length of 512 bits in an encrypted TLS session.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Schannel Information Disclosure Vulnerability (3061518)`
OID:1.3.6.1.4.1.25623.1.0.805552
Version used: `2023-07-25T05:05:58Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-1716
url: https://support.microsoft.com/en-us/kb/3061518
url: http://www.securityfocus.com/bid/74489
url: https://technet.microsoft.com/library/security/MS15-055
cert-bund: CB-K15/0668
dfn-cert: DFN-CERT-2015-0689
```

Medium (CVSS: 5.0)
NVT: Microsoft SHA-2 Code Sign Support Defense in Depth (KB4474419)

Summary
This host is missing a defense-in-depth update according to Microsoft KB4474419

Vulnerability Detection Result

```
Vulnerable range:   Less than 6.1.7601.24382
File checked:       C:\Windows\system32\Crypt32.dll
File version:       6.1.7601.18741
```

Impact
Successful exploitation will allow an attacker to bypass defense-in-depth measures and perform exploitation.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 for 32-bit/x64 Systems Service Pack 1 and
- Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1

Vulnerability Insight
Microsoft has released an update for SHA-2 code signing that introduces SHA-2 code sign support for Windows 7 SP1, and Windows Server 2008 R2 SP1.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft SHA-2 Code Sign Support Defense in Depth (KB4474419)`
OID:1.3.6.1.4.1.25623.1.0.814764
Version used: `2020-06-04T09:02:37Z`

References

```
url: https://support.microsoft.com/en-us/help/4474419
```

Medium (CVSS: 5.0)
NVT: Microsoft Windows IIS FTP Service Information Disclosure Vulnerability (2761226)

Summary
This host is missing a moderate security update according to Microsoft Bulletin MS12-073.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow an attacker to gain access to sensitive information that may aid in further attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft FTP Service 7.0 for IIS 7.0 on Microsoft Windows Vista/2008 server Service Pack 2 and prior
- Microsoft FTP Service 7.5 for IIS 7.5 on:
- Microsoft Windows Vista/2008 server Service Pack 2 and prior
- Microsoft Windows 7 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 Service Pack 1 and prior

Vulnerability Insight
The flaws are due to
- IIS improperly manages the permissions of a log file.
- An error within the IIS FTP service when negotiating encrypted communications channels.

Vulnerability Detection Method
Details: `Microsoft Windows IIS FTP Service Information Disclosure Vulnerability (2761226)`
OID:1.3.6.1.4.1.25623.1.0.902694
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2012-2531
cve: CVE-2012-2532
url: http://support.microsoft.com/kb/2733829
url: http://www.securityfocus.com/bid/56440
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms
↪12-073
dfn-cert: DFN-CERT-2012-2112
```

Medium (CVSS: 5.0)
NVT: Microsoft Windows Search Component Denial of Service Vulnerability (3165270)

Summary
This host is missing an important security update according to Microsoft Bulletin MS16-082

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Structuredquery.dll
File version:     7.0.7601.17514
Vulnerable range: Less than 7.0.7601.23451
```

Impact
Successful exploitation will allow an attacker to potentially escalate permissions or perform additional privileged actions on the target machine.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64

Vulnerability Insight
The flaw is due to the search component fails to properly handle certain objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Search Component Denial of Service Vulnerability (3165270)`
OID:1.3.6.1.4.1.25623.1.0.808163
Version used: `2023-07-21T05:05:22Z`

References

```
cve: CVE-2016-3230
url: https://support.microsoft.com/en-us/kb/3161958
url: https://technet.microsoft.com/library/security/MS16-082
cert-bund: CB-K16/0914
```

Medium (CVSS: 5.0)
NVT: Microsoft .NET Framework Denial of Service Vulnerability (2990931)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing an important security update according to Microsoft Bulletin MS14-053.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to cause a denial of service.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 1.1, 2.0, 3.0, 3.5, 3.5.1, 4.0, 4.5, 4.5.1 and 4.5.2.

Vulnerability Insight

The flaw is due to an error within a hash generation function when hashing requests and can be exploited to cause a hash collision resulting in high CPU consumption via specially crafted requests.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Denial of Service Vulnerability (2990931)`

OID:1.3.6.1.4.1.25623.1.0.804480

Version used: `2023-07-27T05:05:08Z`

References

```
cve: CVE-2014-4072
url: https://technet.microsoft.com/library/security/MS14-053
url: http://www.securityfocus.com/bid/69603
cert-bund: CB-K14/1121
```

Medium (CVSS: 5.0)

NVT: Microsoft Windows OLE Privilege Elevation Vulnerability (3072633)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-075.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to bypass security protections on affected systems.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

The flaw is due to Microsoft Windows incorrectly handles OLE objects in documents.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows OLE Privilege Elevation Vulnerability (3072633)`
OID:1.3.6.1.4.1.25623.1.0.805677
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2015-2416
cve: CVE-2015-2417
url: https://support.microsoft.com/en-us/kb/3072633
url: https://technet.microsoft.com/library/security/MS15-075
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1060
```

Medium (CVSS: 4.9)
NVT: Microsoft Windows Ancillary Function Driver Information Disclosure Vulnerability (2875783)

Summary

This host is missing an important security update according to Microsoft Bulletin MS13-093

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow disclosure of potentially sensitive information if an attacker logs on to a user's system and runs a specially crafted application.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2012
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
The flaw is due an error in Ancillary Function Driver (AFD) which does not properly copies data from kernel memory to user memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Ancillary Function Driver Information Disclosure Vulnerabilit.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.903501
Version used: `2022-07-26T10:10:42Z`

References
```
cve: CVE-2013-3887
url: http://support.microsoft.com/kb/2875783
url: http://www.securityfocus.com/bid/63545
url: https://technet.microsoft.com/en-us/security/bulletin/ms13-093
cert-bund: CB-K13/0909
dfn-cert: DFN-CERT-2013-1921
```

Medium (CVSS: 4.9)
NVT: Microsoft Windows Kerberos Local Security Bypass Vulnerability (3105256)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-122.

Vulnerability Detection Result
```
File checked:     C:\Windows\system32\Kerberos.dll
File version:     6.1.7601.18741
Vulnerable range: Less than 6.1.7601.19043
```

Impact
Successful exploitation will allow local attackers to bypass certain security restrictions and perform unauthorized actions.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Service Pack 1

Vulnerability Insight
The flaw is due to Kerberos fails to check the password change of a user signing into a workstation.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Kerberos Local Security Bypass Vulnerability (3105256)`
OID:1.3.6.1.4.1.25623.1.0.806556
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-6095
url: https://support.microsoft.com/en-us/kb/3105256
url: https://technet.microsoft.com/library/security/MS15-122
cert-bund: CB-K15/1649
dfn-cert: DFN-CERT-2015-1742
```

Medium (CVSS: 4.9)
NVT: Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2778344)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-016.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow remote attackers to a specially crafted program to exploit race conditions in 'win32k.sys' and gain System level privileges.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows XP x32 Edition Service Pack 3 and prior
- Microsoft Windows XP x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
The flaws due to an error in 'win32k.sys' when handling kernel-mode driver objects in memory.

Vulnerability Detection Method
Details: `Microsoft Windows Kernel-Mode Drivers Privilege Elevation Vulnerabilities (2778.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902943
Version used: `2022-05-25T07:40:23Z`

References

```
cve: CVE-2013-1248
cve: CVE-2013-1249
cve: CVE-2013-1250
cve: CVE-2013-1264
cve: CVE-2013-1251
cve: CVE-2013-1265
cve: CVE-2013-1252
cve: CVE-2013-1266
cve: CVE-2013-1253
cve: CVE-2013-1267
cve: CVE-2013-1254
cve: CVE-2013-1255
cve: CVE-2013-1256
cve: CVE-2013-1257
cve: CVE-2013-1258
cve: CVE-2013-1259
cve: CVE-2013-1260
cve: CVE-2013-1261
cve: CVE-2013-1262
cve: CVE-2013-1263
cve: CVE-2013-1268
cve: CVE-2013-1269
cve: CVE-2013-1270
cve: CVE-2013-1271
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-1272
cve: CVE-2013-1273
cve: CVE-2013-1274
cve: CVE-2013-1275
cve: CVE-2013-1276
cve: CVE-2013-1277
url: http://support.microsoft.com/kb/2778344
url: http://www.securityfocus.com/bid/57786
url: http://www.securityfocus.com/bid/57791
url: http://www.securityfocus.com/bid/57792
url: http://www.securityfocus.com/bid/57793
url: http://www.securityfocus.com/bid/57794
url: http://www.securityfocus.com/bid/57795
url: http://www.securityfocus.com/bid/57796
url: http://www.securityfocus.com/bid/57797
url: http://www.securityfocus.com/bid/57798
url: http://www.securityfocus.com/bid/57799
url: http://www.securityfocus.com/bid/57800
url: http://www.securityfocus.com/bid/57801
url: http://www.securityfocus.com/bid/57802
url: http://www.securityfocus.com/bid/57803
url: http://www.securityfocus.com/bid/57804
url: http://www.securityfocus.com/bid/57805
url: http://www.securityfocus.com/bid/57806
url: http://www.securityfocus.com/bid/57807
url: http://www.securityfocus.com/bid/57808
url: http://www.securityfocus.com/bid/57809
url: http://www.securityfocus.com/bid/57810
url: http://www.securityfocus.com/bid/57811
url: http://www.securityfocus.com/bid/57812
url: http://www.securityfocus.com/bid/57813
url: http://www.securityfocus.com/bid/57814
url: http://www.securityfocus.com/bid/57815
url: http://www.securityfocus.com/bid/57816
url: http://www.securityfocus.com/bid/57817
url: http://www.securityfocus.com/bid/57818
url: http://www.securityfocus.com/bid/57819
url: http://www.securitytracker.com/id/1028124
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms
↪13-016
cert-bund: CB-K14/0283
dfn-cert: DFN-CERT-2013-0288
```

Medium (CVSS: 4.8)
NVT: Oracle Java SE Security Updates - 04 - (cpujul2020) - Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some accessible data as well as unauthorized read access to a subset of accessible data.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u251 (1.8.0.251) and earlier, 11.0.7 and earlier, 14.0.1 and earlier on Windows.

Vulnerability Insight

Multiple flaws exist due to errors in the components 'Libraries' and '2D'.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Updates - 04 - (cpujul2020) - Windows`

OID:1.3.6.1.4.1.25623.1.0.118168

Version used: `2024-02-26T14:36:40Z`

References

```
cve: CVE-2020-14556
cve: CVE-2020-14581
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1522
cert-bund: CB-K20/1075
cert-bund: CB-K20/0715
dfn-cert: DFN-CERT-2020-1762
dfn-cert: DFN-CERT-2020-1531
```

Medium (CVSS: 4.8)

NVT: Oracle Java SE Security Updates - 04 - (cpujul2020) - Windows

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some accessible data as well as unauthorized read access to a subset of accessible data.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u251 (1.8.0.251) and earlier, 11.0.7 and earlier, 14.0.1 and earlier on Windows.

Vulnerability Insight

Multiple flaws exist due to errors in the components 'Libraries' and '2D'.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Oracle Java SE Security Updates - 04 - (cpujul2020) - Windows

OID:1.3.6.1.4.1.25623.1.0.118168

Version used: 2024-02-26T14:36:40Z

References

cve: CVE-2020-14556
cve: CVE-2020-14581
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1522
cert-bund: CB-K20/1075
cert-bund: CB-K20/0715
dfn-cert: DFN-CERT-2020-1762
dfn-cert: DFN-CERT-2020-1531

Medium (CVSS: 4.3)
NVT: Microsoft .NET Framework Security Bypass Vulnerability (2984625)

Summary

This host is missing an important security update according to Microsoft Bulletin MS14-046.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation could allow an attacker to execute of arbitrary code and bypass certain security mechanism.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 2.0 Service Pack 2, 3.0 Service Pack 2, 3.5, 3.5.1.

Vulnerability Insight

Flaw is triggered when handling specially crafted website content due to the Address Space Layout Randomization (ASLR) security feature.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Security Bypass Vulnerability (2984625)`

OID:1.3.6.1.4.1.25623.1.0.804740

Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-4062
url: https://technet.microsoft.com/en-us/security/bulletin/ms14-046
url: http://www.securityfocus.com/bid/69145
url: http://support.microsoft.com/kb/2984625
cert-bund: CB-K14/1013
```

Medium (CVSS: 4.3)

NVT: Microsoft Windows XML Core Services Security Feature Bypass Vulnerability (3046482)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-039.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to bypass security restrictions and gain access to sensitive user information.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Flaw exists due to some unspecified error in XML Core services that may allow a context-dependent attacker to bypass the same-origin policy.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows XML Core Services Security Feature Bypass Vulnerability (3046.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.805533
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-1646
url: https://support.microsoft.com/kb/3046482
url: https://technet.microsoft.com/library/security/MS15-039
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545
```

Medium (CVSS: 4.3)
NVT: Microsoft Windows NETLOGON Spoofing Vulnerability (3002657)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-027.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote man-in-the-middle attacker to conduct SMB relay attacks on domain environments utilizing SMB Signing enforcement, and decrypt SMB3 communications intercepted.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2012/R2
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight

Flaw is due to Netlogon service improperly establishes a secure communications channel belonging to a different machine with a spoofed computer name.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows NETLOGON Spoofing Vulnerability (3002657)`
OID:1.3.6.1.4.1.25623.1.0.805145
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0005
url: https://support.microsoft.com/kb/3002657
url: https://technet.microsoft.com/library/security/MS15-027
cert-bund: CB-K15/0319
dfn-cert: DFN-CERT-2015-0324
```

Medium (CVSS: 4.3)
NVT: Microsoft Windows XML Core Services Information Disclosure Vulnerability (3080129)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-084.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to conduct man-in-the-middle (MiTM) attack and gain access to sensitive data.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64

. . . continues on next page . . .

. . . continued from previous page . . .

- Microsoft Windows Server 2012
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight

Flaw exists due to:

- An error in Microsoft XML Core Services which allows forceful use of Secure Sockets Layer (SSL) 2.0.
- An error in Microsoft XML Core Services which exposes memory addresses not intended for public disclosure.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows XML Core Services Information Disclosure Vulnerability (30801.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.805950

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-2434
cve: CVE-2015-2471
cve: CVE-2015-2440
url: https://support.microsoft.com/en-us/kb/3076895
url: http://www.securityfocus.com/bid/76232
url: http://www.securityfocus.com/bid/76257
url: http://www.securityfocus.com/bid/76229
url: https://support.microsoft.com/en-us/kb/3080129
url: https://technet.microsoft.com/library/security/ms15-084
cert-bund: CB-K15/1174
dfn-cert: DFN-CERT-2015-1236
```

Medium (CVSS: 4.3)
NVT: Microsoft DES Encryption Security Advisory (3057154)

Summary

This host is missing an important security update according to Microsoft advisory (3057154).

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to break certain authentication scenarios.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
An update is available that provides enhanced user protection in environments where DES is still enabled for application compatibility reasons.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft DES Encryption Security Advisory (3057154)`
OID:1.3.6.1.4.1.25623.1.0.805678
Version used: `2023-07-25T05:05:58Z`

References
```
url: https://support.microsoft.com/en-us/kb/3057154
url: https://technet.microsoft.com/library/security/3057154
```

Medium (CVSS: 4.3)
NVT: Oracle Java SE Security Update (jul2021) 01 - Windows

Summary
This host is missing a security update according to Oracle.

Vulnerability Detection Result
```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on integrity and confidentiality.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 7u301 (1.7.0.301) and earlier, 8u291 (1.8.0.291) and earlier, 11.0.11 and earlier, 16.0.1 and earlier on Windows.

Vulnerability Insight

Multiple flaws are due to multiple errors in 'Libraries' and 'Networking' components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2021) 01 - Windows`

OID:1.3.6.1.4.1.25623.1.0.818168

Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2021-2341
cve: CVE-2021-2369
url: https://www.oracle.com/security-alerts/cpujul2021.html#AppendixJAVA
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-0464
cert-bund: WID-SEC-2022-0024
cert-bund: CB-K22/0675
cert-bund: CB-K22/0239
cert-bund: CB-K21/0981
cert-bund: CB-K21/0783
dfn-cert: DFN-CERT-2022-1247
dfn-cert: DFN-CERT-2022-0366
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
dfn-cert: DFN-CERT-2022-0074
```

Medium (CVSS: 4.3)

NVT: Oracle Java SE Security Update (jul2021) 01 - Windows

Summary

This host is missing a security update according to Oracle.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attacker to have an impact on integrity and confidentiality.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 7u301 (1.7.0.301) and earlier, 8u291 (1.8.0.291) and earlier, 11.0.11 and earlier, 16.0.1 and earlier on Windows.

Vulnerability Insight
Multiple flaws are due to multiple errors in 'Libraries' and 'Networking' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jul2021) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818168
Version used: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2021-2341
cve: CVE-2021-2369
url: https://www.oracle.com/security-alerts/cpujul2021.html#AppendixJAVA
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-0464
cert-bund: WID-SEC-2022-0024
cert-bund: CB-K22/0675
cert-bund: CB-K22/0239
cert-bund: CB-K21/0981
cert-bund: CB-K21/0783
dfn-cert: DFN-CERT-2022-1247
dfn-cert: DFN-CERT-2022-0366
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
dfn-cert: DFN-CERT-2022-0074
```

Medium (CVSS: 4.3)
NVT: Microsoft Windows XML Core Services Information Disclosure Vulnerability (4010321)

Summary
This host is missing an important security update according to Microsoft Bulletin MS17-022.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\msxml3.dll
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
File version:     8.110.7601.17514
Vulnerable range: Less than 8.110.7601.23648
```

Impact

Successful exploitation will allow remote attackers to test for the presence of files on disk.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 x32/x64
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Server 2016 x64

Vulnerability Insight

Flaw exists due to improper handling of objects in memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows XML Core Services Information Disclosure Vulnerability (40103.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.810623

Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2017-0022
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/help/4010321
url: https://technet.microsoft.com/library/security/MS17-022
cert-bund: CB-K17/0443
dfn-cert: DFN-CERT-2017-0451
```

Medium (CVSS: 4.3)
NVT: Microsoft Graphics Component Information Disclosure Vulnerability (3029944)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is missing an important security update according to Microsoft Bulletin MS15-016.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to disclose certain sensitive information.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2

Vulnerability Insight

Flaw is due to improper handling uninitialized memory when parsing certain, specially crafted TIFF image format files.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Graphics Component Information Disclosure Vulnerability (3029944)`

OID:1.3.6.1.4.1.25623.1.0.805137

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0061
url: https://support.microsoft.com/kb/3029944
url: http://www.securityfocus.com/bid/72456
url: https://technet.microsoft.com/library/security/MS15-016
cert-bund: CB-K15/0171
dfn-cert: DFN-CERT-2015-0175
```

Medium (CVSS: 4.3)

NVT: Microsoft Cryptographic Cipher Suite Prioritization Advisory (3042058)

Summary

This host is missing an important security update according to Microsoft advisory (3042058).

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\schannel.dll
File version:     6.1.7601.18741
Vulnerable range: Version Less than - 6.1.7601.18812
```

Impact

Successful exploitation will allow attackers to break certain authentication scenarios.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2012 R2
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight

An update is available that improves effectiveness of encryption in Windows operating systems by adding cipher suites to the default list on affected systems and thus improving cipher suite priority ordering.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Cryptographic Cipher Suite Prioritization Advisory (3042058)`

OID:1.3.6.1.4.1.25623.1.0.806091

Version used: `2023-07-25T05:05:58Z`

References

```
url: https://support.microsoft.com/en-us/kb/3042058
url: https://technet.microsoft.com/library/security/3042058
```

Medium (CVSS: 4.3)

NVT: Microsoft JScript and VBScript Scripting Engines Information Disclosure Vulnerability (2475792)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS11-009.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow remote attackers to gain access to sensitive information that may aid in further attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
The flaw is caused by a memory corruption error in the JScript and VBScript scripting engines when processing scripts in Web pages.

Vulnerability Detection Method
Details: `Microsoft JScript and VBScript Scripting Engines Information Disclosure Vulnera.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902336
Version used: `2022-05-25T07:40:23Z`

References
```
cve: CVE-2011-0031
url: http://www.vupen.com/english/advisories/2011/0322
url: http://www.securityfocus.com/bid/46139
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms
↪11-009
```

Medium (CVSS: 4.3)
NVT: Microsoft Windows Command Line Parameter Information Disclosure Vulnerability (3082458)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-088.

Vulnerability Detection Result
```
File checked:     C:\Windows\system32\Notepad.exe
File version:     6.1.7601.17514
Vulnerable range: Less than 6.1.7601.18918
```

Impact
Successful exploitation will allow a local attacker to obtain sensitive information that may aid in further attacks.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight
The flaw is due to an improper security restrictions on files stored on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Command Line Parameter Information Disclosure Vulnerability (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.806012
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-2423
url: https://support.microsoft.com/en-us/kb/3046017
url: http://www.securityfocus.com/bid/76202
url: https://support.microsoft.com/en-us/kb/3079757
url: https://technet.microsoft.com/library/security/MS15-088
cert-bund: CB-K15/1174
cert-bund: CB-K15/1172
cert-bund: CB-K15/1169
dfn-cert: DFN-CERT-2015-1236
dfn-cert: DFN-CERT-2015-1235
dfn-cert: DFN-CERT-2015-1231
```

Medium (CVSS: 4.3)
NVT: Microsoft .NET Framework Privilege Elevation Vulnerabilities (3104507)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-118.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
File checked:     C:\Windows\Microsoft.NET\Framework64\v2.0.50727\System.Deploym
↪ent.dll
File version:     2.0.50727.5420
Vulnerable range: Less than 2.0.50727.5493
```

Impact

Successful exploitation will allow an attacker to gain read access to local files, bypass the security feature and then load additional malicious code, inject client-side script into a users browser and ultimately modify or spoof content, conduct phishing activities, disclose information, or perform any action on the vulnerable website that the target user has permission to perform.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5, 4.5.1, and 4.5.2
- Microsoft .NET Framework 4.6, 4.6 RC

Vulnerability Insight

Multiple flaws exist due to:

- An error in the .NET Framework DTD parsing of certain specially crafted XML files.
- ASP.NET improperly validates values in HTTP requests.
- An error in the .NET Framework component which does not properly implement the Address Space Layout Randomization (ASLR) security feature.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework Privilege Elevation Vulnerabilities (3104507)`

OID:1.3.6.1.4.1.25623.1.0.806614

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-6096
cve: CVE-2015-6099
cve: CVE-2015-6115
url: https://support.microsoft.com/en-us/kb/3104507
url: https://technet.microsoft.com/library/security/MS15-118
cert-bund: CB-K15/1656
dfn-cert: DFN-CERT-2015-1740
```

Medium (CVSS: 4.3)
NVT: Microsoft Windows Photo Decoder Information Disclosure Vulnerability (3035126)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-029.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to gain access to potentially sensitive information in memory.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior
- Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Flaw exists due to error in the Photo decoder that is triggered as the program fails to handle uninitialized memory when parsing a specially crafted JPEG XR image

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Photo Decoder Information Disclosure Vulnerability (3035126)`
OID:1.3.6.1.4.1.25623.1.0.805501
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-0076
url: https://support.microsoft.com/kb/3035126
url: https://technet.microsoft.com/library/security/MS15-029
cert-bund: CB-K15/0319
dfn-cert: DFN-CERT-2015-0324
```

Medium (CVSS: 4.3)
NVT: Microsoft Schannel Security Feature Bypass Vulnerability (3046049)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-031.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attacker to conduct cipher-downgrade attacks to EXPORT_RSA ciphers via crafted TLS traffic.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 2003 x32/x64 Service Pack 2
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2

Vulnerability Insight
The flaw is due to an error in schannel which does not properly restrict TLS state transitions.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Schannel Security Feature Bypass Vulnerability (3046049)`
OID:1.3.6.1.4.1.25623.1.0.805490
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1637
url: https://support.microsoft.com/kb/3046049
url: http://www.securityfocus.com/bid/72965
url: https://technet.microsoft.com/library/security/ms15-031
cert-bund: CB-K15/0319
cert-bund: CB-K15/0290
dfn-cert: DFN-CERT-2015-0324
dfn-cert: DFN-CERT-2015-0300
```

Medium (CVSS: 4.3)
NVT: Microsoft PNG Processing Information Disclosure Vulnerability (3035132)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-024.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow remote attacker to access sensitive information that could be used to launch additional attacks.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 x32 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x64 Service Pack 2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/2012R2

Vulnerability Insight
The flaw is due to improper memory operations performed by the affected software when handling crafted content

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft PNG Processing Information Disclosure Vulnerability (3035132)`
OID:1.3.6.1.4.1.25623.1.0.805489
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-0080
url: https://support.microsoft.com/kb/3035132
url: https://technet.microsoft.com/library/security/ms15-024
url: https://technet.microsoft.com/library/security/MS15-024
cert-bund: CB-K15/0319
dfn-cert: DFN-CERT-2015-0324
```

Medium (CVSS: 4.2)
NVT: Oracle Java SE Security Update (cpuoct2020 - 01) - Windows

Summary
Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 7u271 (1.7.0.271) and earlier, 8u261 (1.8.0.261) and earlier, 11.0.8 and earlier, 15.

Vulnerability Insight
Multiple flaws are due to errors in components Libraries, JSSE, Hotspot, Serialization and JNDI.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (cpuoct2020 - 01) - Windows`
OID:1.3.6.1.4.1.25623.1.0.817610
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2020-14792
cve: CVE-2020-14781
cve: CVE-2020-14782
cve: CVE-2020-14797
cve: CVE-2020-14779
cve: CVE-2020-14796
cve: CVE-2020-14798
url: https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-2242
cert-bund: WID-SEC-2022-1285
cert-bund: CB-K21/0927
cert-bund: CB-K21/0279
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K20/1014
dfn-cert: DFN-CERT-2020-2682
dfn-cert: DFN-CERT-2020-2290
```

Medium (CVSS: 4.2)
NVT: Oracle Java SE Security Update (cpuoct2020 - 01) - Windows

Summary
Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 7u271 (1.7.0.271) and earlier, 8u261 (1.8.0.261) and earlier, 11.0.8 and earlier, 15.

Vulnerability Insight
Multiple flaws are due to errors in components Libraries, JSSE, Hotspot, Serialization and JNDI.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (cpuoct2020 - 01) - Windows`
OID:1.3.6.1.4.1.25623.1.0.817610
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2020-14792
cve: CVE-2020-14781
cve: CVE-2020-14782
cve: CVE-2020-14797
cve: CVE-2020-14779
cve: CVE-2020-14796
cve: CVE-2020-14798
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-2242
cert-bund: WID-SEC-2022-1285
cert-bund: CB-K21/0927
cert-bund: CB-K21/0279
cert-bund: CB-K20/1014
dfn-cert: DFN-CERT-2020-2682
dfn-cert: DFN-CERT-2020-2290
```

Medium (CVSS: 4.0)
NVT: Microsoft Internet Explorer Information Disclosure and Web Site Spoofing Vulnerabilities

Summary
Microsoft Internet Explorer is prone to information disclosure and web site spoofing vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation allows attackers to disclose the sensitive information and view the contents of spoofed site or carry out phishing attacks.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
Microsoft Internet Explorer versions 8 and 9.

Vulnerability Insight
The proxy settings configuration has same proxy address and value for HTTP and HTTPS,
- TCP session to proxy sever will not properly be reused. This allows remote attackers to steal cookie information via crafted HTML document.
- SSl lock consistency with address bar is not ensured. This allows remote attackers to spoof web sites via a crafted HTML document.

Vulnerability Detection Method
Details: `Microsoft Internet Explorer Information Disclosure and Web Site Spoofing Vulner.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.803305
Version used: `2024-06-21T05:05:42Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2013-1450
cve: CVE-2013-1451
url: http://pastebin.com/raw.php?i=rz9BcBey
url: http://www.securityfocus.com/bid/57640
url: http://www.securityfocus.com/bid/57641
url: http://cxsecurity.com/cveshow/CVE-2013-1450
url: http://cxsecurity.com/cveshow/CVE-2013-1451
url: http://www.security-database.com/detail.php?alert=CVE-2013-1450
url: http://www.security-database.com/detail.php?alert=CVE-2013-1451
```

Medium (CVSS: 4.0)
NVT: Microsoft Windows Active Directory Service Denial of Service Vulnerability (3072595)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-096.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Samsrv.dll
File version:     6.1.7601.17514
Vulnerable range: 6.1.7601.18000 - 6.1.7601.18956
```

Impact

Successful exploitation will allow an the attacker to cause the service to become non-responsive, resulting in denial-of-service conditions.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior

Vulnerability Insight

The flaw is due to improper resource management by the affected software while creating multiple machine accounts.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Active Directory Service Denial of Service Vulnerability (307.`
`↪..`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.806044
Version used: 2023-07-25T05:05:58Z

References

```
cve: CVE-2015-2535
url: https://support.microsoft.com/en-us/kb/3072595
url: https://technet.microsoft.com/library/security/MS15-096
cert-bund: CB-K15/1321
dfn-cert: DFN-CERT-2015-1385
```

[return to 192.168.56.103]

2.1.15 Medium 9200/tcp

Medium (CVSS: 6.8)
NVT: Elasticsearch Remote Code Execution Vulnerability

Summary

Elasticsearch is prone to a remote-code-execution vulnerability.

Vulnerability Detection Result

```
Vulnerable URL: http://192.168.56.103:9200/_search?source=%7B%22size%22%3A1%2C%2
↪2query%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match_all%22%3A%7B%7D%7
↪D%7D%7D%2C%22script_fields%22%3A%7B%22VTTest%22%3A%7B%22script%22%3A%22import%
↪20java.util.*%3B%5Cnimport%20java.io.*%3B%5Cnnew%20Scanner(new%20File(%5C%22%2
↪Fwindows%2Fwin.ini%5C%22)).useDelimiter(%5C%22%5C%5C%5CZ%5C%22).next()%3B%2
↪2%7D%7D%7D&callback=?
```

Impact

An attacker can exploit this issue to execute arbitrary code

Solution:

Solution type: VendorFix

Ask the vendor for an update or disable 'dynamic scripting'

Affected Software/OS

Elasticsearch < 1.2

Vulnerability Insight

Elasticsearch has a flaw in its default configuration which makes it possible for any webpage to execute arbitrary code on visitors with Elasticsearch installed.

Vulnerability Detection Method

Send a special crafted HTTP GET request and check the response

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Elastisearch Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105032
Version used: `2023-07-27T05:05:08Z`

References

```
cve: CVE-2014-3120
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://bouk.co/blog/elasticsearch-rce/
cert-bund: CB-K14/1131
```

Medium (CVSS: 6.5)
NVT: Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerability - Windows

Summary
Elasticsearch is prone to a field disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     6.8.12
Installation
path / port:       /
```

Impact
An attacker could gain additional permissions against a restricted index.

Solution:
Solution type: VendorFix
Update to version 6.8.12, 7.9.1 or later.

Affected Software/OS
Elasticsearch prior to version 6.8.12 and 7.9.0.

Vulnerability Insight
A field disclosure flaw was found in Elasticsearch when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerabilit.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.144431
Version used: `2024-02-15T05:05:40Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2020-7019
url: https://discuss.elastic.co/t/elastic-stack-7-9-0-and-6-8-12-security-update
↪/245456
```

Medium (CVSS: 6.5)
NVT: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)

Summary

Elasticsearch is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     6.8.17
Installation
path / port:       /
```

Solution:

Solution type: VendorFix

Update to version 6.8.17, 7.13.3 or later.

Affected Software/OS

Elasticsearch prior to version 6.8.17 and 7.x prior to 7.13.3.

Vulnerability Insight

An uncontrolled recursion vulnerability that could lead to a denial of service attack was identified in the Elasticsearch Grok parser. A user with the ability to submit arbitrary queries to Elasticsearch could create a malicious Grok query that will crash the Elasticsearch node.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)`

OID:1.3.6.1.4.1.25623.1.0.146386

Version used: `2021-08-17T12:00:57Z`

References

```
cve: CVE-2021-22144
url: https://discuss.elastic.co/t/elasticsearch-7-13-3-and-6-8-17-security-updat
↪e/278100
cert-bund: WID-SEC-2022-1777
dfn-cert: DFN-CERT-2022-2315
```

Medium (CVSS: 5.9)
NVT: Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability (ESA-2019-07) - Windows

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     6.8.2
Installation
path / port:       /
```

Impact
On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.

Solution:
Solution type: VendorFix
Update to version 6.8.2 or 7.2.1 respectively.

Affected Software/OS
Elasticsearch through version 6.8.1 and version 7.0.0 through 7.2.0.

Vulnerability Insight
A race condition flaw was found in the response headers Elasticsearch returns to a request.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117162
Version used: `2024-02-19T05:05:57Z`

References

```
cve: CVE-2019-7614
url: https://discuss.elastic.co/t/elastic-stack-6-8-2-and-7-2-1-security-update/
↪192963
url: https://www.elastic.co/community/security/
```

Medium (CVSS: 5.3)
NVT: Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)

Summary
Elasticsearch is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     6.8.15
Installation
path / port:       /
```

Impact

This could lead to disclosing the existence of documents and fields the attacker should not be able to view or result in an attacker gaining additional insight into potentially sensitive indices.

Solution:

Solution type: VendorFix

Update to version 6.8.15, 7.12.0 or later.

Affected Software/OS

Elasticsearch versions prior to versions 6.8.15 or 7.12.0.

Vulnerability Insight

The following vulnerabilities exist:

- CVE-2021-22135: Suggester & Profile API information disclosure flaw
- CVE-2021-22137: Field disclosure flaw

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)`

OID:1.3.6.1.4.1.25623.1.0.145940

Version used: `2021-08-17T12:00:57Z`

References

```
cve: CVE-2021-22135
cve: CVE-2021-22137
url: https://discuss.elastic.co/t/elastic-stack-7-12-0-and-6-8-15-security-updat
↪e/268125
cert-bund: WID-SEC-2022-0720
```

Medium (CVSS: 4.9)

NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)

Summary

Elasticsearch is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     6.8.14
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        /
```

Impact
This could allow an Elasticsearch administrator to view sensitive details.

Solution:
Solution type: VendorFix
Update to version 6.8.14, 7.10.0 or later.

Affected Software/OS
Elasticsearch versions prior to 6.8.14 and 7.0.0 prior to 7.10.0.

Vulnerability Insight
Elasticsearch has an information disclosure issue when audit logging and the emit_request_body option is enabled. The Elasticsearch audit log could contain sensitive information such as password hashes or authentication tokens.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)`
OID:1.3.6.1.4.1.25623.1.0.145383
Version used: `2021-08-17T12:00:57Z`

References

```
cve: CVE-2020-7021
url: https://discuss.elastic.co/t/elastic-stack-7-11-0-and-6-8-14-security-updat
↪e/263915
url: https://www.elastic.co/community/security
```

Medium (CVSS: 4.3)
NVT: Elasticsearch Cross-site Scripting (XSS) Vulnerability - Windows

Summary
Elasticsearch is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     1.4.0.Beta1
```

Impact
Successful exploitation will allow remote attackers to inject arbitrary web script or HTML.

Solution:
Solution type: VendorFix
Update to Elasticsearch version 1.4.0.Beta1, or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Elasticsearch version 1.3.x and prior on Windows.

Vulnerability Insight
The Flaw is due to an error in the CORS functionality.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elasticsearch Cross-site Scripting (XSS) Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.808092
Version used: `2024-02-15T05:05:40Z`

References

```
cve: CVE-2014-6439
url: https://www.elastic.co/community/security/
url: http://www.securityfocus.com/bid/70233
url: http://www.securityfocus.com/archive/1/archive/1/533602/100/0/threaded
```

[return to 192.168.56.103]

2.1.16 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Password required for anonymous.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: `FTP Unencrypted Cleartext Login`

OID:1.3.6.1.4.1.25623.1.0.108528

Version used: `2023-12-20T05:05:58Z`

[return to 192.168.56.103]

2.1.17 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

Solution:

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak

. . . continues on next page . . .

... continued from previous page ...

- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

References

```
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=metasploitable3-win2k8
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

. . . continues on next page . . .

. . . continued from previous page . . .

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

References

```
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-
↪sha-1-based-signature-algorithms/
```

[return to 192.168.56.103]

2.1.18 Medium 3306/tcp

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.28
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.1.66, 5.5.28 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle MySQL Server versions 5.1.65 and prior and 5.5 through 5.5.27.

Vulnerability Insight
The flaw allows remote authenticated users to affect availability, related to GIS Extension.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117201
Version used: `2021-02-12T11:09:59Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2012-5060
url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL
advisory-id: cpujan2013
dfn-cert: DFN-CERT-2013-0079
```

Medium (CVSS: 6.8)
NVT: MySQL Server Components Multiple Unspecified Vulnerabilities

Product detection result
```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.5.20-log
Fixed version:     See advisory
```

Impact
Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
MySQL version 5.1.x before 5.1.62 and 5.5.x before 5.5.22.

Vulnerability Insight
Multiple unspecified errors exist in the Server Optimizer and Server DML components.

Vulnerability Detection Method
Details: `MySQL Server Components Multiple Unspecified Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.803808
Version used: `2023-07-27T05:05:08Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-1690
cve: CVE-2012-1688
cve: CVE-2012-1703
url: http://secunia.com/advisories/48890
url: http://www.securityfocus.com/bid/53058
url: http://www.securityfocus.com/bid/53067
url: http://www.securityfocus.com/bid/53074
url: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#Ap
↪pendixMSQL
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1170
dfn-cert: DFN-CERT-2012-0939
dfn-cert: DFN-CERT-2012-0936
dfn-cert: DFN-CERT-2012-0933
dfn-cert: DFN-CERT-2012-0735
```

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server Multiple Vulnerabilities - 02 - (Nov 2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪25623.1.0.100152)
```

Summary
Oracle MySQL server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the references or upgrade to latest version.

Affected Software/OS
Oracle MySQL version 5.1.x to 5.1.65 and Oracle MySQL version 5.5.x to 5.5.27 on Windows.

Vulnerability Insight
The flaws are due to multiple unspecified errors in MySQL server component related to server installation and server optimizer.

Vulnerability Detection Method
Details: `Oracle MySQL Server Multiple Vulnerabilities - 02 - (Nov 2012) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803112
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-3180
cve: CVE-2012-3177
cve: CVE-2012-3160
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56003
url: http://www.securityfocus.com/bid/56005
url: http://www.securityfocus.com/bid/56027
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://support.oracle.com/rs?type=doc&id=1475188.1
dfn-cert: DFN-CERT-2012-2200
dfn-cert: DFN-CERT-2012-2118
```

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.29
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.5.29 or later.

Affected Software/OS

Oracle MySQL Server versions 5.5 through 5.5.28.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows`

OID:1.3.6.1.4.1.25623.1.0.117205

Version used: `2021-02-12T11:09:59Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-5612
cve: CVE-2013-0386
cve: CVE-2013-0368
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-0371
cve: CVE-2012-0578
cve: CVE-2013-0367
cve: CVE-2012-5096
url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL
advisory-id: cpujan2013
dfn-cert: DFN-CERT-2013-0259
dfn-cert: DFN-CERT-2013-0079
```

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server 5.5.x <= 5.5.23 Security Update (cpujul2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.24
Installation
path / port:       3306/tcp
```

Impact
The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'InnoDB' package / privilege.

Solution:
Solution type: VendorFix
Update to version 5.5.24 or later.

Affected Software/OS
Oracle MySQL Server 5.5.x through 5.5.23.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server 5.5.x <= 5.5.23 Security Update (cpujul2012) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117267
Version used: `2021-03-18T11:53:07Z`

Product Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-1735
cve: CVE-2012-1757
cve: CVE-2012-1756
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2012-1389
```

Medium (CVSS: 6.7)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote to have an impact on availability, confidentiality and integrity.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.53 and earlier, 5.6.34 and earlier, 5.7.16 and earlier on Windows

Vulnerability Insight

Multiple flaws exist due to: multiple unspecified errors in sub components ’Error Handling’, ’Logging’, ’MyISAM’, ’Packaging’, ’Optimizer’, ’DML’ and ’DDL’.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.809865

Version used: `2023-11-03T05:05:46Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2017-3238
cve: CVE-2017-3318
cve: CVE-2017-3291
cve: CVE-2017-3317
cve: CVE-2017-3258
cve: CVE-2017-3312
cve: CVE-2017-3313
cve: CVE-2017-3244
cve: CVE-2017-3265
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/95571
url: http://www.securityfocus.com/bid/95560
url: http://www.securityfocus.com/bid/95491
url: http://www.securityfocus.com/bid/95527
url: http://www.securityfocus.com/bid/95565
url: http://www.securityfocus.com/bid/95588
url: http://www.securityfocus.com/bid/95501
url: http://www.securityfocus.com/bid/95585
url: http://www.securityfocus.com/bid/95520
cert-bund: CB-K18/0224
cert-bund: CB-K17/1732
cert-bund: CB-K17/1604
cert-bund: CB-K17/1298
cert-bund: CB-K17/0927
cert-bund: CB-K17/0423
cert-bund: CB-K17/0098
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0959
dfn-cert: DFN-CERT-2017-0430
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0090
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Security Update (cpujul2018 - 02) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See reference
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle MySQL version 5.5.60 and earlier, 5.6.40 and earlier, 5.7.22 and earlier.

Vulnerability Insight

Multiple flaws exist due to errors in 'Server: Security: Encryption', 'Server: Options', 'MyISAM', 'Client mysqldump' components of application.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Security Update (cpujul2018 - 02) - Windows`

OID:1.3.6.1.4.1.25623.1.0.813706

Version used: `2023-11-03T16:10:08Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2018-2767
cve: CVE-2018-3066
cve: CVE-2018-3058
cve: CVE-2018-3070
url: https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL
advisory-id: cpujul2018
cert-bund: WID-SEC-2023-1594
cert-bund: CB-K18/0795
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2018-1649
dfn-cert: DFN-CERT-2018-1402
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0913
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.38 / 5.6 <= 5.6.19 Security Update (cpuoct2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.39
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Update to version 5.5.39, 5.6.20 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5.38 and prior and 5.6 through 5.6.19.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to CLIENT:MYSQLADMIN, CLIENT:MYSQLDUMP, SERVER:MEMORY STORAGE ENGINE, SERVER:SSL:yaSSL, SERVER:DML, SERVER:SSL:yaSSL, SERVER:REPLICATION ROW FORMAT BINARY LOG DML, SERVER:CHARACTER SETS, and SERVER:MyISAM.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.38 / 5.6 <= 5.6.19 Security Update (cpuoct2014) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804782
Version used: `2021-02-12T11:09:59Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2014-6530
cve: CVE-2012-5615
cve: CVE-2014-6495
cve: CVE-2014-6478
cve: CVE-2014-4274
cve: CVE-2014-4287
cve: CVE-2014-6484
cve: CVE-2014-6505
cve: CVE-2014-6463
cve: CVE-2014-6551
url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL
advisory-id: cpuoct2014
cert-bund: CB-K15/1518
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K14/1482
cert-bund: CB-K14/1420
cert-bund: CB-K14/1412
cert-bund: CB-K14/1299
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2013-0259
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.31 and prior and 5.6 through 5.6.11.

Vulnerability Insight
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.806878
Version used: `2022-09-12T10:18:03Z`

Product Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-0502
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81136
advisory-id: cpujan2016
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0094
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.31
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Update to version 5.1.69, 5.5.31, 5.6.11 or later.

Affected Software/OS

Oracle MySQL Server versions 5.1.68 and prior, 5.5 through 5.5.30 and 5.6 through 5.6.10.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Unspecified error in Server Optimizer, Server Privileges, InnoDB, and in some unspecified vectors.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.117207

Version used: `2022-07-21T10:11:30Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-2375
cve: CVE-2013-1544
cve: CVE-2013-1532
cve: CVE-2013-2389
cve: CVE-2013-2392
cve: CVE-2013-2391
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59207
url: http://www.securityfocus.com/bid/59209
url: http://www.securityfocus.com/bid/59224
url: http://www.securityfocus.com/bid/59242
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpuapr2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     5.7.33
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.33, 8.0.23 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.32 and prior and 8.0 through 8.0.22.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpuapr2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145794
Version used: `2023-10-20T16:09:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2020-1971
cve: CVE-2021-2178
cve: CVE-2021-2202
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0067
cert-bund: WID-SEC-2023-0065
cert-bund: WID-SEC-2022-2047
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1000
cert-bund: WID-SEC-2022-0585
cert-bund: CB-K21/1065
cert-bund: CB-K21/0788
cert-bund: CB-K21/0615
cert-bund: CB-K21/0421
cert-bund: CB-K21/0111
cert-bund: CB-K21/0062
cert-bund: CB-K21/0006
cert-bund: CB-K20/1217
dfn-cert: DFN-CERT-2022-1582
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2020-2791
dfn-cert: DFN-CERT-2020-2668
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 02 (May 2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.36 and earlier and 5.6.16 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Performance Schema, Options, RBR.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 02 (May 2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.804575
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2014-2430
cve: CVE-2014-2431
cve: CVE-2014-2436
cve: CVE-2014-2440
url: http://secunia.com/advisories/57940
url: http://www.securityfocus.com/bid/66850
url: http://www.securityfocus.com/bid/66858
url: http://www.securityfocus.com/bid/66890
url: http://www.securityfocus.com/bid/66896
url: http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638
url: http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0464
cert-bund: CB-K14/0452
```

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple denial of service (DoS) vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of these vulnerabilities will allow remote attackers to conduct a denial-of-service attack.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.20 and earlier on Windows

Vulnerability Insight

Multiple flaws exist due to:

- An error in the 'Server: DDL' component.

- Multiple errors in the 'Server: Optimizer' component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.812646

Version used: `2024-02-29T14:37:57Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2018-2668
cve: CVE-2018-2665
cve: CVE-2018-2622
cve: CVE-2018-2640
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0480
cert-bund: CB-K18/0392
cert-bund: CB-K18/0265
cert-bund: CB-K18/0096
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0424
dfn-cert: DFN-CERT-2018-0286
dfn-cert: DFN-CERT-2018-0101
```

Medium (CVSS: 6.5)

NVT: Oracle MySQL Server <= 5.6.49 / 5.7 <= 5.7.31 / 8.0 <= 8.0.21 Security Update (cpuoct2020) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.50
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.50, 5.7.32, 8.0.22 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.49 and prior, 5.7 through 5.7.31 and 8.0 through 8.0.21.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.49 / 5.7 <= 5.7.31 / 8.0 <= 8.0.21 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.108959
Version used: `2021-08-16T12:00:57Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2020-14765
cve: CVE-2020-14769
cve: CVE-2020-14812
cve: CVE-2020-14793
cve: CVE-2020-14672
cve: CVE-2020-14867
url: https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixMSQL
advisory-id: cpuoct2020
cert-bund: CB-K20/1066
cert-bund: CB-K20/1017
dfn-cert: DFN-CERT-2020-2763
dfn-cert: DFN-CERT-2020-2756
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2380
```

. . . continues on next page . . .

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2020-2295

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.46 Security Update (cpujan2020) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.47
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.6.47 or later.

Affected Software/OS

Oracle MySQL Server versions 5.6.46 and prior.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.6.46 Security Update (cpujan2020) - Windows`

OID:1.3.6.1.4.1.25623.1.0.143359

Version used: `2021-08-16T09:00:57Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2020-2579
url: https://www.oracle.com/security-alerts/cpujan2020.html#AppendixMSQL
advisory-id: cpujan2020
cert-bund: CB-K20/0038
dfn-cert: DFN-CERT-2020-1827
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-0096
```

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to compromise availability of the system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.11 and earlier on Windows.

Vulnerability Insight

The flaw exists due to an error in 'Server: Optimizer'

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.811986

Version used: `2023-07-25T05:05:58Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2017-10378
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101375
cert-bund: CB-K18/0480
cert-bund: CB-K18/0242
cert-bund: CB-K18/0224
cert-bund: CB-K17/2048
cert-bund: CB-K17/1748
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0260
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-2137
dfn-cert: DFN-CERT-2017-1827
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (cpuoct2019) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.46
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.6.46, 5.7.28, 8.0.18 or later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle MySQL Server versions 5.6.45 and prior, 5.7 through 5.7.27 and 8.0 through 8.0.17.

Vulnerability Insight

Oracle MySQL Server is prone to multiple vulnerabilities.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143030
Version used: `2021-09-07T14:01:38Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2019-2974
cve: CVE-2019-2911
url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL
advisory-id: cpuoct2019
cert-bund: CB-K20/1030
cert-bund: CB-K20/0109
cert-bund: CB-K19/0915
dfn-cert: DFN-CERT-2020-2763
dfn-cert: DFN-CERT-2020-2756
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2180
dfn-cert: DFN-CERT-2020-1827
dfn-cert: DFN-CERT-2020-0658
dfn-cert: DFN-CERT-2020-0517
dfn-cert: DFN-CERT-2020-0103
dfn-cert: DFN-CERT-2019-2695
dfn-cert: DFN-CERT-2019-2687
dfn-cert: DFN-CERT-2019-2656
dfn-cert: DFN-CERT-2019-2301
dfn-cert: DFN-CERT-2019-2149
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 (Jul 2014) - Windows

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.37 and earlier and 5.6.17 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to SRINFOSC and SRCHAR.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-02 (Jul 2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.804722
Version used: `2024-02-16T05:06:55Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2014-4258
cve: CVE-2014-4260
url: http://secunia.com/advisories/59521
url: http://www.securityfocus.com/bid/68564
url: http://www.securityfocus.com/bid/68573
url: http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_securi
↪ty_patches
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#A
↪ppendixMSQL
cert-bund: CB-K15/0567
cert-bund: CB-K14/1420
cert-bund: CB-K14/0891
cert-bund: CB-K14/0868
dfn-cert: DFN-CERT-2015-0593
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (cpujul2019) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.45
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.6.45, 5.7.27, 8.0.17 or later.

Affected Software/OS

Oracle MySQL Server versions 5.6.44 and prior, 5.7 through 5.7.26 and 8.0 through 8.0.16.

Vulnerability Insight

Oracle MySQL Server is prone to multiple denial of service vulnerabilities.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.142645
Version used: `2023-10-27T16:11:32Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2019-2805
cve: CVE-2019-2740
cve: CVE-2019-2819
cve: CVE-2019-2739
cve: CVE-2019-2737
cve: CVE-2019-2738
url: https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL
advisory-id: cpujul2019
cert-bund: CB-K19/0620
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2180
dfn-cert: DFN-CERT-2020-0658
dfn-cert: DFN-CERT-2020-0517
dfn-cert: DFN-CERT-2019-2695
dfn-cert: DFN-CERT-2019-2656
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2008
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1683
dfn-cert: DFN-CERT-2019-1568
dfn-cert: DFN-CERT-2019-1453
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Oracle MySQL Server versions 5.5.51 and prior.

Vulnerability Insight

The flaw exists due to an unspecified error within the 'Server:DML' component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows`

OID:1.3.6.1.4.1.25623.1.0.809378

Version used: `2022-07-21T10:11:30Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-5624
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K16/1846
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
```

Medium (CVSS: 6.5)

NVT: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.30
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Update to version 5.1.68, 5.5.30, 5.6.11 or later.

Affected Software/OS

Oracle MySQL Server versions 5.1.67 and prior, 5.5 through 5.5.29 and 5.6 through 5.6.10.

Vulnerability Insight

Unspecified error in some unknown vectors related to Information Schema.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 / 5.6 <= 5.6.10 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.117206

Version used: `2022-07-21T10:11:30Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-2378
cve: CVE-2013-1506
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59188
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798
```

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote to compromise availability confidentiality, and integrity of the system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.19 and earlier on Windows.

Vulnerability Insight

Multiple flaws exist due to:

- An error in 'Client programs' component.
- An error in 'Server: DDL'.
- An error in 'Server: Replication'

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows`

OID:1.3.6.1.4.1.25623.1.0.811991

Version used: `2023-11-03T05:05:46Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2017-10379
cve: CVE-2017-10384
cve: CVE-2017-10268
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101415
url: http://www.securityfocus.com/bid/101406
url: http://www.securityfocus.com/bid/101390
cert-bund: CB-K18/0480
cert-bund: CB-K18/0242
cert-bund: CB-K18/0224
cert-bund: CB-K17/2048
cert-bund: CB-K17/1748
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0260
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-2137
dfn-cert: DFN-CERT-2017-1827
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpuapr2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.29
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.1.67, 5.5.29 or later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpuapr2013) - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.803459

Version used: `2022-07-21T10:11:30Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-1531
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798
```

Medium (CVSS: 6.5)

NVT: Oracle MySQL Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (cpuoct2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.50 and prior, 5.6 through 5.6.31 and 5.7 through 5.7.13.

Vulnerability Insight
The flaw exists due to an unspecified error in the 'Server: DML' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809374
Version used: `2022-07-21T10:11:30Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-5612
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K16/1979
cert-bund: CB-K16/1755
cert-bund: CB-K16/1742
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.5.20
Fixed version:     5.5.30
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Update to version 5.1.68, 5.5.30 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.67 and prior and 5.5 through 5.5.29.

Vulnerability Insight
Unspecified error in Server Partition and in some unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117209
Version used: `2022-04-25T14:50:49Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2013-1521
cve: CVE-2013-1552
cve: CVE-2013-1555
cve: CVE-2012-5614
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59196
url: http://www.securityfocus.com/bid/59210
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798
```

Medium (CVSS: 6.4)
NVT: Oracle MySQL Server Multiple Vulnerabilities - 04 - (Nov 2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data, and cause a DoS (Denial of Service).

Solution:

Solution type: VendorFix

Apply the patch from the referenced vendor advisory or upgrade to the latest version.

Affected Software/OS

Oracle MySQL version 5.5.x to 5.5.26 on Windows.

Vulnerability Insight

The flaws are due to multiple unspecified errors in MySQL server component vectors related to MySQL client and server.

Vulnerability Detection Method

Details: `Oracle MySQL Server Multiple Vulnerabilities - 04 - (Nov 2012) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803114
Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-3147
cve: CVE-2012-3149
cve: CVE-2012-3144
url: http://secunia.com/advisories/51008/
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/56006
url: http://www.securityfocus.com/bid/56008
url: http://www.securityfocus.com/bid/56022
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
cert-bund: CB-K13/0919
dfn-cert: DFN-CERT-2013-1937
```

Medium (CVSS: 6.2)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (cpuoct2019) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a local unauthenticated vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.45
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.6.45, 5.7.27, 8.0.17 or later.

Affected Software/OS

Oracle MySQL Server versions 5.6.44 and prior, 5.7 through 5.7.26 and 8.0 through 8.0.16.

Vulnerability Insight

Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.143032

Version used: `2021-09-08T08:01:40Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2019-2969
url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL
advisory-id: cpuoct2019
cert-bund: CB-K19/0915
dfn-cert: DFN-CERT-2019-2149
```

Medium (CVSS: 6.1)
NVT: Oracle MySQL Server <= 5.5.47 / 5.6 <= 5.6.28 / 5.7 <= 5.7.10 Security Update (cpuapr2016v3) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.47 and prior, 5.6 through 5.6.28 and 5.7 through 5.7.10.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.5.47 / 5.6 <= 5.6.28 / 5.7 <= 5.7.10 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.807928

Version used: `2023-11-03T05:05:46Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-0649
cve: CVE-2016-0650
cve: CVE-2016-0644
cve: CVE-2016-0646
cve: CVE-2016-0640
cve: CVE-2016-0641
url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL
advisory-id: cpuapr2016v3
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0750
cert-bund: CB-K16/0646
cert-bund: CB-K16/0597
```

Medium (CVSS: 5.9)

NVT: Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (cpuapr2019) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     5.6.44
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.44, 5.7.26, 8.0.16 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.43 and prior, 5.7 through 5.7.25 and 8.0 through 8.0.15.

Vulnerability Insight
The attacks range in variety and difficulty. Most of them allow an attacker with network access via multiple protocols to compromise the MySQL Server.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.142403
Version used: `2022-03-28T03:06:01Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2019-1559
cve: CVE-2019-2683
cve: CVE-2019-2627
cve: CVE-2019-2614
url: https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL
advisory-id: cpuapr2019
cert-bund: WID-SEC-2023-2946
cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0462
cert-bund: CB-K22/0045
cert-bund: CB-K20/0041
cert-bund: CB-K19/0911
cert-bund: CB-K19/0639
cert-bund: CB-K19/0623
cert-bund: CB-K19/0622
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K19/0620
cert-bund: CB-K19/0619
cert-bund: CB-K19/0615
cert-bund: CB-K19/0332
cert-bund: CB-K19/0320
cert-bund: CB-K19/0319
cert-bund: CB-K19/0173
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2189
dfn-cert: DFN-CERT-2020-2180
dfn-cert: DFN-CERT-2020-0092
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2625
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2274
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2157
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-2008
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1755
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1683
dfn-cert: DFN-CERT-2019-1678
dfn-cert: DFN-CERT-2019-1677
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1486
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1453
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-0968
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0566
dfn-cert: DFN-CERT-2019-0556
dfn-cert: DFN-CERT-2019-0412
```

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (cpuapr2019) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a vulnerability in the libmysqld subcomponent.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.43
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.6.43, 5.7.25, 8.0.14 or later.

Affected Software/OS

Oracle MySQL Server versions 5.6.42 and prior, 5.7 through 5.7.24 and 8.0 through 8.0.13.

Vulnerability Insight

Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.142405

Version used: `2021-09-07T14:01:38Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2018-3123
url: https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory-id: cpuapr2019
cert-bund: WID-SEC-2023-1594
cert-bund: CB-K19/0319
dfn-cert: DFN-CERT-2019-0775
```

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpujul2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.43
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.43, 8.0.34 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.33.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpujul2023) - Win.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.149981

Version used: `2023-10-13T05:06:10Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2023-22053
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL
advisory-id: cpujul2023
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-1794
dfn-cert: DFN-CERT-2024-1188
dfn-cert: DFN-CERT-2024-0593
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0454
dfn-cert: DFN-CERT-2023-1642
```

Medium (CVSS: 5.9)
NVT: Oracle MySQL Backronym Vulnerability (Jun 2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to the backronym vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.3
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack.

Solution:

Solution type: VendorFix

Upgrade to version Oracle MySQL Server 5.7.3 or later.

Affected Software/OS

Oracle MySQL Server 5.7.2 and earlier on Windows.

Vulnerability Insight

The flaw exists due to improper validation of MySQL client library when establishing a secure connection to a MySQL server using the –ssl option.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Oracle MySQL Backronym Vulnerability (Jun 2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.808063
Version used: 2024-02-16T05:06:55Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2015-3152
url: http://www.ocert.org/advisories/ocert-2015-003.html
url: https://duo.com/blog/backronym-mysql-vulnerability
cert-bund: CB-K18/0871
cert-bund: CB-K16/0944
cert-bund: CB-K15/1045
cert-bund: CB-K15/1042
cert-bund: CB-K15/1020
cert-bund: CB-K15/0994
cert-bund: CB-K15/0964
cert-bund: CB-K15/0895
dfn-cert: DFN-CERT-2015-1105
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071
dfn-cert: DFN-CERT-2015-1051
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0942

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpuapr2016v3) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

`path / port:        3306/tcp`

Impact

Successful exploitation will allow remote users to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.

Vulnerability Insight

Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.807924

Version used: `2023-11-03T05:05:46Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-0666
cve: CVE-2016-0647
cve: CVE-2016-0648
cve: CVE-2016-0642
cve: CVE-2016-0643
cve: CVE-2016-2047
url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL
advisory-id: cpuapr2016v3
cert-bund: CB-K16/1129
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0750
cert-bund: CB-K16/0646
cert-bund: CB-K16/0597
cert-bund: CB-K16/0493
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0133
```

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to a vulnerability in a third party library.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
The flaw makes it easier for remote attackers to obtain private RSA keys by capturing TLS handshakes, aka a Lenstra attack.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.45 and prior and 5.6 through 5.6.26.

Vulnerability Insight
wolfSSL (formerly CyaSSL) as used in MySQL does not properly handle faults associated with the Chinese Remainder Theorem (CRT) process when allowing ephemeral key exchange without low memory optimizations on a server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117194
Version used: `2022-08-31T10:10:28Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-7744
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
advisory-id: cpujan2016
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0094
```

Medium (CVSS: 5.7)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 (Apr 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to cause a denial of service.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Server : Optimizer, DDL, Server : Compiling, Server : Federated.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-03 (Apr 2015) - Windows
OID:1.3.6.1.4.1.25623.1.0.805172
Version used: 2024-02-09T05:06:25Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2015-2571
cve: CVE-2015-0505
cve: CVE-2015-0501
cve: CVE-2015-0499
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74095
url: http://www.securityfocus.com/bid/74112
url: http://www.securityfocus.com/bid/74070
url: http://www.securityfocus.com/bid/74115
cert-bund: WID-SEC-2023-2068
cert-bund: CB-K15/1546
cert-bund: CB-K15/1518
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1042
cert-bund: CB-K15/0964
cert-bund: CB-K15/0720
cert-bund: CB-K15/0531
dfn-cert: DFN-CERT-2015-1623
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1105
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0551

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow local users to affect availability.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.46 and prior.

Vulnerability Insight
Unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Optimizer'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows`
OID:1.3.6.1.4.1.25623.1.0.807922
Version used: `2022-08-31T10:10:28Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-0651
url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL
advisory-id: cpuapr2016v3
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0597
```

Medium (CVSS: 5.4)
NVT: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.29
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.1.67, 5.5.29 or later.

Affected Software/OS

Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpujan2013) - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.117203

Version used: `2023-11-02T05:05:26Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-5611
cve: CVE-2013-0384
cve: CVE-2013-0389
cve: CVE-2013-0385
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-0375
cve: CVE-2012-1702
cve: CVE-2013-0383
cve: CVE-2012-0572
cve: CVE-2012-0574
cve: CVE-2012-1705
cve: CVE-2012-4414
url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL
advisory-id: cpujan2013
cert-bund: CB-K13/0919
cert-bund: CB-K13/0603
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-1597
dfn-cert: DFN-CERT-2013-0259
dfn-cert: DFN-CERT-2013-0192
dfn-cert: DFN-CERT-2013-0119
dfn-cert: DFN-CERT-2013-0118
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2013-0079
dfn-cert: DFN-CERT-2013-0037
dfn-cert: DFN-CERT-2013-0028
dfn-cert: DFN-CERT-2012-2285
dfn-cert: DFN-CERT-2012-2258
dfn-cert: DFN-CERT-2012-2215
dfn-cert: DFN-CERT-2012-2200
```

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.40
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 5.7.40, 8.0.31 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.30.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.118388
Version used: `2022-10-24T10:14:58Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2022-2097
cve: CVE-2022-21617
cve: CVE-2022-21608
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-1777
cert-bund: WID-SEC-2022-1776
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1146
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-1065
cert-bund: WID-SEC-2022-0561
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2491
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-1058
dfn-cert: DFN-CERT-2023-0509
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2323
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-2315
dfn-cert: DFN-CERT-2022-2306
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1536
dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1515
dfn-cert: DFN-CERT-2022-1497
```

Medium (CVSS: 5.3)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 03 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to a security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to bypass certain security restrictions and perform unauthorized actions by conducting a man-in-the-middle attack. This may lead to other attacks also.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier on Windows

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The flaw exists due to an incorrect implementation or enforcement of 'ssl-mode=REQUIRED' in MySQL.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (apr2017-3236618) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.810884
Version used: `2023-07-25T05:05:58Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2017-3305
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97023
cert-bund: CB-K17/1604
cert-bund: CB-K17/1239
cert-bund: CB-K17/0657
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675
```

Medium (CVSS: 5.3)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to partially access data, partially modify data, and partially deny service.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, on Windows

Vulnerability Insight
The flaw exists due to an error in the Client programs component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811434
Version used: `2024-02-29T14:37:57Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2017-3636
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
↪#AppendixMSQL
url: http://www.securityfocus.com/bid/99736
cert-bund: CB-K18/0224
cert-bund: CB-K17/1870
cert-bund: CB-K17/1604
cert-bund: CB-K17/1453
cert-bund: CB-K17/1401
cert-bund: CB-K17/1239
cert-bund: CB-K17/1205
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1956
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1519
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243
```

Medium (CVSS: 5.3)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, 5.7.18 and earlier, on Windows

Vulnerability Insight

Multiple flaws exist due to
- A flaw in the Client mysqldump component.
- A flaw in the Server: DDL component.
- A flaw in the C API component.
- A flaw in the Connector/C component.
- A flaw in the Server: Charsets component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811432
Version used: `2024-02-29T14:37:57Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2017-3651
cve: CVE-2017-3653
cve: CVE-2017-3652
cve: CVE-2017-3635
cve: CVE-2017-3648
cve: CVE-2017-3641
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
↪#AppendixMSQL
url: http://www.securityfocus.com/bid/99802
url: http://www.securityfocus.com/bid/99810
url: http://www.securityfocus.com/bid/99805
url: http://www.securityfocus.com/bid/99730
url: http://www.securityfocus.com/bid/99789
url: http://www.securityfocus.com/bid/99767
cert-bund: CB-K18/0224
cert-bund: CB-K17/1870
cert-bund: CB-K17/1732
cert-bund: CB-K17/1604
cert-bund: CB-K17/1453
cert-bund: CB-K17/1401
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/1205
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1956
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1519
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243
```

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities in OpenSSL.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.47
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.47, 5.7.27 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.46 and prior and 5.7 through 5.7.26.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143735
Version used: `2021-08-16T09:00:57Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2019-1547
cve: CVE-2019-1549
cve: CVE-2019-1552
cve: CVE-2019-1563
url: https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixMSQL
advisory-id: cpuapr2020
cert-bund: WID-SEC-2023-3081
cert-bund: WID-SEC-2023-1762
cert-bund: WID-SEC-2023-1049
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049
cert-bund: CB-K20/1016
cert-bund: CB-K20/0321
cert-bund: CB-K20/0318
cert-bund: CB-K20/0043
cert-bund: CB-K20/0038
cert-bund: CB-K20/0036
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K20/0028
cert-bund: CB-K19/1025
cert-bund: CB-K19/0919
cert-bund: CB-K19/0915
cert-bund: CB-K19/0808
cert-bund: CB-K19/0675
dfn-cert: DFN-CERT-2023-2709
dfn-cert: DFN-CERT-2020-2014
dfn-cert: DFN-CERT-2020-1729
dfn-cert: DFN-CERT-2020-0895
dfn-cert: DFN-CERT-2020-0776
dfn-cert: DFN-CERT-2020-0775
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2020-0277
dfn-cert: DFN-CERT-2020-0101
dfn-cert: DFN-CERT-2020-0096
dfn-cert: DFN-CERT-2020-0091
dfn-cert: DFN-CERT-2020-0090
dfn-cert: DFN-CERT-2019-2164
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1900
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1559
```

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 Security Update (cpuoct2019) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.46
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.46, 5.7.28 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle MySQL Server versions 5.6.45 and prior and 5.7 through 5.7.27.

Vulnerability Insight
Oracle MySQL Server is prone to multiple vulnerabilities.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 Security Update (cpuoct2019) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143034
Version used: `2021-09-08T08:01:40Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2019-2922
cve: CVE-2019-2923
cve: CVE-2019-2924
cve: CVE-2019-2910
url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL
advisory-id: cpuoct2019
cert-bund: CB-K19/0915
dfn-cert: DFN-CERT-2020-0103
dfn-cert: DFN-CERT-2019-2149
```

Medium (CVSS: 5.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 (Apr 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to cause a denial of service.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier on windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to DDL, Server : Security : Privileges, Server : Security : Encryption, InnoDB : DML.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified vulnerabilities-02 (Apr 2015) - Windows`

OID:1.3.6.1.4.1.25623.1.0.805171

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-2573
cve: CVE-2015-2568
cve: CVE-2015-0441
cve: CVE-2015-0433
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74078
url: http://www.securityfocus.com/bid/74073
url: http://www.securityfocus.com/bid/74103
url: http://www.securityfocus.com/bid/74089
cert-bund: WID-SEC-2023-2068
cert-bund: CB-K15/1546
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K15/1042
cert-bund: CB-K15/0964
cert-bund: CB-K15/0720
cert-bund: CB-K15/0531
dfn-cert: DFN-CERT-2015-1623
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1105
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0551
```

Medium (CVSS: 5.0)
NVT: MySQL Unspecified vulnerabilities-03 (Jul 2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL 5.5.30 and earlier and 5.6.10 on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Prepared Statements, Server Options and Server Partition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `MySQL Unspecified vulnerabilities-03 (Jul 2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803725
Version used: `2024-02-20T14:37:13Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-3801
cve: CVE-2013-3805
cve: CVE-2013-3794
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61222
url: http://www.securityfocus.com/bid/61256
url: http://www.securityfocus.com/bid/61269
cert-bund: CB-K13/0919
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Security Update (cpujul2018 - 04) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See reference
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle MySQL version 5.5.60 and earlier.

Vulnerability Insight
Multiple flaws exist due to an error in the 'Server: Security: Privileges' component of MySQL Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Security Update (cpujul2018 - 04) - Windows`
OID:1.3.6.1.4.1.25623.1.0.813710
Version used: `2022-08-22T10:11:10Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2018-3063
url: https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL
advisory-id: cpujul2018
cert-bund: WID-SEC-2023-1594
cert-bund: CB-K18/0795
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2018-1649
dfn-cert: DFN-CERT-2018-1402
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpujan2021) - Windows

Product detection result
```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.51
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.51, 5.7.33, 8.0.23 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.32 and 8.0 through 8.0.22.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145224
Version used: `2021-08-26T13:01:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2021-2022
cve: CVE-2021-2060
url: https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL
advisory-id: cpujan2021
cert-bund: WID-SEC-2023-0067
cert-bund: CB-K21/0062
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.31
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.31, 8.0.18 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.30 and prior and 8.0 through 8.0.17.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145804
Version used: `2021-08-26T13:01:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2021-2160
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2023-0065
cert-bund: CB-K21/0421
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.34
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.34 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.33 and prior.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows`

OID:1.3.6.1.4.1.25623.1.0.145802

Version used: `2021-08-26T13:01:12Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2021-2154
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2023-0065
cert-bund: CB-K21/0421
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0666
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server Component 'Replication' Unspecified vulnerability (Oct 2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL versions 5.5.10 through 5.5.32 and 5.6.x through 5.6.12 on Windows

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Replication.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server Component 'Replication' Unspecified vulnerability (Oct 2013.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804034
Version used: `2024-02-20T14:37:13Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-5807
url: http://secunia.com/advisories/55327
url: http://www.securityfocus.com/bid/63105
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html
cert-bund: CB-K14/0187
cert-bund: CB-K13/1072
cert-bund: CB-K13/0840
cert-bund: CB-K13/0789
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1846
dfn-cert: DFN-CERT-2013-1795
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.43, 8.x <= 8.0.31 Security Update (cpuoct2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.44
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.44, 8.0.32 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.43 and prior and 8.x through 8.0.31.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.43, 8.x <= 8.0.31 Security Update (cpuoct2023) - Win.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.151216

Version used: `2023-10-20T05:06:03Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2023-22028
url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL
advisory-id: cpuoct2023
cert-bund: WID-SEC-2023-2690
dfn-cert: DFN-CERT-2024-0108
dfn-cert: DFN-CERT-2023-2536
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.31 Security Update (cpuoct2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.43
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.43, 8.0.32 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.31.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.31 Security Update (cpuoct2023) - Win.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.151212

Version used: `2023-10-20T05:06:03Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

. . . continues on next page . . .

... continued from previous page ...

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2023-22015
cve: CVE-2023-22026
url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL
advisory-id: cpuoct2023
cert-bund: WID-SEC-2023-2690
dfn-cert: DFN-CERT-2023-2536
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpujul2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.42
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.42, 8.0.33 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.32.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpujul2023) - Win.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.149979

Version used: `2023-10-13T05:06:10Z`

Product Detection Result

... continues on next page ...

. . . continued from previous page . . .

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2023-22007
url: https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL
advisory-id: cpujul2023
cert-bund: WID-SEC-2023-1794
dfn-cert: DFN-CERT-2024-1188
dfn-cert: DFN-CERT-2024-0593
dfn-cert: DFN-CERT-2024-0454
dfn-cert: DFN-CERT-2023-1642
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.40 Security Update (cpujan2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.41
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix
Update to version 5.7.41 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.40 and prior.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.40 Security Update (cpujan2023) - Windows`
OID:1.3.6.1.4.1.25623.1.0.149168
Version used: `2023-10-13T05:06:10Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2023-21840
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL
advisory-id: cpujan2023
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0126
dfn-cert: DFN-CERT-2023-0105
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpujan2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.51
Installation
path / port:       3306/tcp
```

Impact
Successful attacks of this vulnerability can result in the unauthorized ability to cause a hang or frequently repeatedly crash (complete DOS) the MySQL Server.

Solution:
Solution type: VendorFix
Update to version 5.6.51, 5.7.31, 8.0.18 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.30 and 8.0 through 8.0.17.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.145222

Version used: `2021-08-26T13:01:12Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2021-2001
url: https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL
advisory-id: cpujan2021
cert-bund: WID-SEC-2023-0067
cert-bund: CB-K21/0062
```

Medium (CVSS: 4.6)

NVT: Oracle MySQL Server 5.5 <= 5.5.29 / 5.6 <= 5.6.11 Security Update (cpuapr2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.30
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.5.30, 5.6.11 or later.

Affected Software/OS

Oracle MySQL Server versions 5.5 through 5.5.29 and 5.6 through 5.6.10.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server 5.5 <= 5.5.29 / 5.6 <= 5.6.11 Security Update (cpuapr2013) .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117213
Version used: `2021-02-12T11:09:59Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-1523
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0798
```

Medium (CVSS: 4.4)
NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpuoct2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.37
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.37, 8.0.28 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.36 and prior and 8.0 through 8.0.27.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpuoct2022) - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.118382

Version used: `2023-10-19T05:05:21Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2022-21595
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2023-0504
dfn-cert: DFN-CERT-2022-2306
```

Medium (CVSS: 4.4)

NVT: Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote to have some unspecified impact on availability.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle MySQL version 5.5.53 and earlier on Windows

Vulnerability Insight
The flaw exists due to an unspecified error in sub component 'Server: Charsets'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.809869
Version used: `2023-07-25T05:05:58Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2017-3243
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/95538
cert-bund: CB-K18/0224
cert-bund: CB-K17/1298
cert-bund: CB-K17/0098
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0090
```

Medium (CVSS: 4.3)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.29 Security Update (cpuoct2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.40
```

. . . continues on next page . . .

... continued from previous page ...

```
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.40, 8.0.30 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.29.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.29 Security Update (cpuoct2022) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.118386
Version used: `2023-10-19T05:05:21Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2022-21592
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2022-2306
```

Medium (CVSS: 4.3)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Windows

Product detection result
```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 5.5.20
```

... continues on next page ...

. . . continued from previous page . . .

```
Fixed version:     5.7.40
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.40, 8.0.17 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.16.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.118384
Version used: `2023-10-19T05:05:21Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2022-21589
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2022-2306
```

Medium (CVSS: 4.3)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-03 (Jul 2015)

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.43 and earlier and 5.6.23 and earlier on Windows

Vulnerability Insight
Unspecified errors exist in the MySQL Server component via unknown vectors related to Server : Pluggable Auth and Server : Security : Privileges.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-03 (Jul 2015)`
OID:1.3.6.1.4.1.25623.1.0.805930
Version used: `2024-02-20T05:05:48Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-4737
cve: CVE-2015-2620
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75802
url: http://www.securityfocus.com/bid/75837
cert-bund: CB-K15/1518
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1020
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability (Oct 2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL versions 5.1.51 through 5.1.70, 5.5.10 through 5.5.32, and 5.6.x through 5.6.12 on Windows.

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Optimizer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability (Oct 2013) .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804033
Version used: `2024-02-20T14:37:13Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-3839
url: http://secunia.com/advisories/55327
url: http://www.securityfocus.com/bid/63109
url: http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html
cert-bund: CB-K14/0187
cert-bund: CB-K13/1072
cert-bund: CB-K13/0840
cert-bund: CB-K13/0806
cert-bund: CB-K13/0789
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1846
dfn-cert: DFN-CERT-2013-1815
dfn-cert: DFN-CERT-2013-1795
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-08 (Oct 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle MySQL Server 5.5.44 and earlier on windows

Vulnerability Insight

Unspecified error exists in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-08 (Oct 2015) - Windows`

OID:1.3.6.1.4.1.25623.1.0.805771

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-4816
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77134
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K15/1844
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638
```

Medium (CVSS: 4.0)

NVT: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.5.20
Fixed version:     5.5.23
Installation
path / port:       3306/tcp
```

Impact

The flaw allows remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' package / privilege.

Solution:

Solution type: VendorFix

Update to version 5.1.63, 5.5.23 or later.

Affected Software/OS

Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.22.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - .`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.117263

Version used: `2021-03-18T11:53:07Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-1689
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1389
```

Medium (CVSS: 4.0)

NVT: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.24
Installation
path / port:       3306/tcp
```

Impact

The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'GIS Extension' package / privilege.

Solution:

Solution type: VendorFix

Update to version 5.1.63, 5.5.24 or later.

Affected Software/OS

Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.23.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - .`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.117265

Version used: `2021-03-18T11:53:07Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-0540
cve: CVE-2012-1734
cve: CVE-2012-2749
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1389
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.31
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Update to version 5.5.31, 5.6.11 or later.

Affected Software/OS

Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.10.

Vulnerability Insight

Unspecified error in some unknown vectors related to Stored Procedure.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) .`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.809815

Version used: `2022-04-25T14:50:49Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-2376
cve: CVE-2013-1511
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59227
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0798
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.30
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.5.30 or later.

Affected Software/OS

Oracle MySQL Server versions 5.5 through 5.5.29.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows`

OID:1.3.6.1.4.1.25623.1.0.117215

Version used: `2021-02-12T11:09:59Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2013-1512
cve: CVE-2013-1526
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0798
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 03 (Jan 2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.33 and earlier on Windows, Oracle MySQL version 5.6.13 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Partition.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 03 (Jan 2014) - Windows`

OID:1.3.6.1.4.1.25623.1.0.804074

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-5891
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64891
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
```

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerability-06 (Jul 2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL 5.5.31 and earlier on Windows.

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Server Parser.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerability-06 (Jul 2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803728
Version used: `2024-02-20T14:37:13Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-3783
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61210
cert-bund: CB-K13/1072
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478
```

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerabilities-02 (Jul 2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote authenticated users to affect integrity and availability via unknown vectors and cause denial of service.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Oracle MySQL 5.5.31 and earlier, 5.6.11 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Server Replication, Audit Log and Data Manipulation Language.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerabilities-02 (Jul 2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803724
Version used: `2024-02-20T14:37:13Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-3812
cve: CVE-2013-3809
cve: CVE-2013-3793
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61249
url: http://www.securityfocus.com/bid/61264
url: http://www.securityfocus.com/bid/61272
cert-bund: CB-K13/1072
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478
```

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerabilities-01 (Jul 2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

MySQL is prone to multiple unspecified vulnerabilities.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, 5.6.11 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Full Text Search and Server Optimizer.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerabilities-01 (Jul 2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803723
Version used: `2024-02-20T14:37:13Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-3804
cve: CVE-2013-3802
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61244
url: http://www.securityfocus.com/bid/61260
cert-bund: CB-K13/1072
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 04 (Jan 2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to InnoDB, Optimizer, Error Handling, and some unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 04 (Jan 2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.804075
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2014-0401
cve: CVE-2014-0412
cve: CVE-2014-0437
cve: CVE-2013-5908
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64849
url: http://www.securityfocus.com/bid/64880
url: http://www.securityfocus.com/bid/64896
url: http://www.securityfocus.com/bid/64898
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K15/1518
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0177
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
dfn-cert: DFN-CERT-2015-1604
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 05 (Jan 2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Optimizer, InnoDB, and Locking.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 05 (Jan 2014) - Windows`

OID:1.3.6.1.4.1.25623.1.0.804076

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2014-0386
cve: CVE-2014-0393
cve: CVE-2014-0402
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64877
url: http://www.securityfocus.com/bid/64904
url: http://www.securityfocus.com/bid/64908
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0177
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
```

Medium (CVSS: 4.0)

NVT: Oracle MySQL Server Multiple Vulnerabilities - 03 - (Nov 2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data.

Solution:
Solution type: VendorFix
Apply the patch from the referenced vendor advisory or upgrade to latest version.

Affected Software/OS
Oracle MySQL version 5.1.x to 5.1.63 and Oracle MySQL version 5.5.x to 5.5.25 on Windows.

Vulnerability Insight
The flaws are due to multiple unspecified errors in MySQL server component vectors related to InnoDB plugin, server full text search and InnoDB.

Vulnerability Detection Method
Details: `Oracle MySQL Server Multiple Vulnerabilities - 03 - (Nov 2012) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803113
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-3173
cve: CVE-2012-3167
cve: CVE-2012-3166
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56018
url: http://www.securityfocus.com/bid/56028
url: http://www.securityfocus.com/bid/56041
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
dfn-cert: DFN-CERT-2012-2200
dfn-cert: DFN-CERT-2012-2118
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-01 (Oct 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
```

... continues on next page ...

... continued from previous page ...

```
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier on windows

Vulnerability Insight
Unspecified errors exist in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-01 (Oct 2015) - Windows`
OID:1.3.6.1.4.1.25623.1.0.805764
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-4913
cve: CVE-2015-4830
cve: CVE-2015-4826
cve: CVE-2015-4815
cve: CVE-2015-4807
cve: CVE-2015-4802
cve: CVE-2015-4792
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2015-4870
cve: CVE-2015-4861
cve: CVE-2015-4858
cve: CVE-2015-4836
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77153
url: http://www.securityfocus.com/bid/77228
url: http://www.securityfocus.com/bid/77237
url: http://www.securityfocus.com/bid/77222
url: http://www.securityfocus.com/bid/77205
url: http://www.securityfocus.com/bid/77165
url: http://www.securityfocus.com/bid/77171
url: http://www.securityfocus.com/bid/77208
url: http://www.securityfocus.com/bid/77137
url: http://www.securityfocus.com/bid/77145
url: http://www.securityfocus.com/bid/77190
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K15/1844
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

. . . continues on next page . . .

... continued from previous page ...

Impact

Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Oracle MySQL Server versions 5.5.46 and prior and 5.6 through 5.6.27.

Vulnerability Insight

Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.806877

Version used: `2022-04-13T13:17:10Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-0596
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81176
url: http://www.securityfocus.com/bid/81198
url: http://www.securityfocus.com/bid/81130
advisory-id: cpujan2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133
cert-bund: CB-K16/0094
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 (Feb 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
```

Impact

Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server version 5.5.40 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Server:InnoDB:DDL:Foreign Key

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified vulnerabilities-02 (Feb 2015) - Windows`

OID:1.3.6.1.4.1.25623.1.0.805133

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-0432
url: http://secunia.com/advisories/62525
url: http://www.securityfocus.com/bid/72217
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K15/1193
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074
```

Medium (CVSS: 4.0)
NVT: MySQL Server Component Partition Unspecified Vulnerability

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20-log
Fixed version:     5.5.22
```

Impact
Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
MySQL version 5.5.x before 5.5.22

Vulnerability Insight
Unspecified error in MySQL Server component related to Partition.

Vulnerability Detection Method
Details: `MySQL Server Component Partition Unspecified Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.803801
Version used: `2024-03-04T14:37:58Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-1697
url: http://secunia.com/advisories/48890
url: http://www.securityfocus.com/bid/53064
url: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#Ap
↪pendixMSQL
dfn-cert: DFN-CERT-2012-0939
dfn-cert: DFN-CERT-2012-0735
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.46 Security Update (cpujan2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.46 and prior.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.46 Security Update (cpujan2016) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117190
Version used: `2021-02-12T11:09:59Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-0616
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
advisory-id: cpujan2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133
cert-bund: CB-K16/0094
```

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerability-04 (Jul 2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier and 5.6.10 on Windows.

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Server Options.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerability-04 (Jul 2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803726
Version used: `2024-02-20T14:37:13Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2013-3808
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61227
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-02 (Jul 2015)

Product detection result
```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to cause denial-of-service attack.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on Windows.

Vulnerability Insight

Unspecified errors exist in the MySQL Server component via unknown vectors related to DML, Server : I_S, Server : Optimizer, and GIS.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-02 (Jul 2015)`

OID:1.3.6.1.4.1.25623.1.0.805929

Version used: `2024-02-20T05:05:48Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-2648
cve: CVE-2015-4752
cve: CVE-2015-2643
cve: CVE-2015-2582
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75822
url: http://www.securityfocus.com/bid/75849
url: http://www.securityfocus.com/bid/75830
url: http://www.securityfocus.com/bid/75751
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1020
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 (Jul 2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20-log
Vulnerable range:  5.5 - 5.5.37
```

Impact

Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.37 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to ENARC and SROPTZR.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified vulnerabilities-03 (Jul 2014) - Windows`

OID:1.3.6.1.4.1.25623.1.0.804723

Version used: `2024-02-16T05:06:55Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2014-2494
cve: CVE-2014-4207
url: http://secunia.com/advisories/59521
url: http://www.securityfocus.com/bid/68579
url: http://www.securityfocus.com/bid/68593
url: http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_securi
↪ty_patches
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#A
↪ppendixMSQL
cert-bund: CB-K15/0567
cert-bund: CB-K14/1420
cert-bund: CB-K14/0891
cert-bund: CB-K14/0868
dfn-cert: DFN-CERT-2015-0593
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.38 Security Update (cpuoct2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.39
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:
Solution type: VendorFix
Update to version 5.5.39 or later.

. . . continues on next page . . .

... continued from previous page ...

Affected Software/OS
Oracle MySQL Server versions 5.5.38 and prior.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to SERVER:DDL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.38 Security Update (cpuoct2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.804783
Version used: `2022-04-14T11:24:11Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2014-6520
url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL
url: http://www.securityfocus.com/bid/70510
advisory-id: cpuoct2014
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K14/1482
cert-bund: CB-K14/1420
cert-bund: CB-K14/1412
cert-bund: CB-K14/1299
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 01 (May 2014) - Windows

Product detection result
```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.35 and earlier and 5.6.15 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Partition, Replication and XML subcomponent.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 01 (May 2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.804574
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2014-0384
cve: CVE-2014-2419
cve: CVE-2014-2438
url: http://secunia.com/advisories/57940
url: http://www.securityfocus.com/bid/66835
url: http://www.securityfocus.com/bid/66846
url: http://www.securityfocus.com/bid/66880
url: http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638
url: http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0464
cert-bund: CB-K14/0452
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-04 (Feb 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
```

Impact

Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server version 5.5.38 and earlier, and 5.6.19 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to DLL.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Multiple Unspecified vulnerabilities-04 (Feb 2015) - Windows`

OID:1.3.6.1.4.1.25623.1.0.805135

Version used: `2024-02-09T05:06:25Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-0391
url: http://secunia.com/advisories/62525
url: http://www.securityfocus.com/bid/72205
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/1193
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074
```

[return to 192.168.56.103]

2.1.19 Medium 3820/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Summary
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.0          | 10
TLSv1.1          | 10
TLSv1.2          | 10
```

Impact
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

. . . continues on next page . . .

. . . continued from previous page . . .

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-02-02T05:06:11Z`

References

```
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
The certificate of the remote service expired on 2023-05-13 05:33:38.
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Impact

An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.

Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`

OID:1.3.6.1.4.1.25623.1.0.113054

Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`

Method: `SSL/TLS: Collect and Report Certificate Details`

OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.1
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`

OID:1.3.6.1.4.1.25623.1.0.117274

Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security:1.1`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References

```
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html
```

[return to 192.168.56.103]

2.1.20 Medium 8383/tcp

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

Summary
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Vulnerability Detection Result

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00F59CEF71E6DB72A5:1.2.840.113549.1.9.1=#737570706F7274406465736B746F70
↪63656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L
↪=Pleasanton,ST=CA,C=US (Server certificate)
```

Impact
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

References
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2020-09-05 12:24:44.
Certificate details:
fingerprint (SHA-1)             | 701E2E6DF8854C4F0B298DFF03A2C6F0BAC7D315
fingerprint (SHA-256)           | C1DF756862FA17582C31E8F8EBDA084D1A1341815B716E
↪B135AD83CD7B01A5A5
issued by                       | 1.2.840.113549.1.9.1=#737570706F7274406465736B
↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora
↪tion,L=Pleasanton,ST=CA,C=US
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00F59CEF71E6DB72A5
signature algorithm             | sha1WithRSAEncryption
subject                         | 1.2.840.113549.1.9.1=#737570706F7274406465736B
↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora
↪tion,L=Pleasanton,ST=CA,C=US
subject alternative names (SAN) | None
valid from                      | 2010-09-08 12:24:44 UTC
valid until                     | 2020-09-05 12:24:44 UTC
```

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

`cpe:/a:ietf:transport_layer_security:1.1`

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.1`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size $<$ 2048).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References

```
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Subject:              1.2.840.113549.1.9.1=#737570706F7274406465736B746F7063656E
↪7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleas
↪anton,ST=CA,C=US
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

or

fingerprint1, Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`

OID:1.3.6.1.4.1.25623.1.0.105880

Version used: `2021-10-15T11:13:32Z`

References

```
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-
↪sha-1-based-signature-algorithms/
```

[return to 192.168.56.103]

2.1.21 Medium 4848/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2023-05-13 05:33:38.
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details: `SSL/TLS: Certificate Expired`

OID:1.3.6.1.4.1.25623.1.0.103955

Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`

Method: `SSL/TLS: Collect and Report Certificate Details`

OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Impact

An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.

Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`

OID:1.3.6.1.4.1.25623.1.0.113054

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.1
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security:1.1`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
```

[return to 192.168.56.103]

2.1.22 Medium 3920/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2023-05-13 05:33:38.
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
valid until                    | 2023-05-13 05:33:38 UTC
```

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details: `SSL/TLS: Certificate Expired`

OID:1.3.6.1.4.1.25623.1.0.103955

Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`

Method: `SSL/TLS: Collect and Report Certificate Details`

OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)

NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)            | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)          | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                      | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm           | RSA
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Impact

An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.

Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`

OID:1.3.6.1.4.1.25623.1.0.113054

Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`

Method: `SSL/TLS: Collect and Report Certificate Details`

OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.1
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.1`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References
```
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html
```

[return to 192.168.56.103]

2.1.23 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: OpenSSH < 7.8 User Enumeration Vulnerability - Windows

Product detection result
```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.1
Fixed version:     7.8
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution:
Solution type: VendorFix
Update to version 7.8 or later.

Affected Software/OS
OpenSSH versions 7.7 and prior.

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH < 7.8 User Enumeration Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813863
Version used: `2023-07-20T05:05:18Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
cve: CVE-2018-15473
url: https://0day.city/cve-2018-15473.html
url: https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d
↪1e0
cert-bund: WID-SEC-2024-1082
cert-bund: CB-K20/0041
cert-bund: CB-K18/1031
cert-bund: CB-K18/0873
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2020-2189
dfn-cert: DFN-CERT-2020-0228
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-0857
dfn-cert: DFN-CERT-2019-0362
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-2293
dfn-cert: DFN-CERT-2018-2259
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-1806
dfn-cert: DFN-CERT-2018-1696
```

Medium (CVSS: 5.3)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     None
Installation
path / port:       22/tcp
```

Impact

Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution:

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

OpenSSH version 5.9 through 7.8.

Vulnerability Insight

The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.813887

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2021-05-28T07:06:21Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
cve: CVE-2018-15919
url: https://bugzilla.novell.com/show_bug.cgi?id=1106163
url: https://seclists.org/oss-sec/2018/q3/180
cert-bund: WID-SEC-2024-1082
cert-bund: CB-K18/0885
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2018-2293
dfn-cert: DFN-CERT-2018-2191
```

Medium (CVSS: 5.3)
NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
openssh is prone to a security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     7.6
Installation
path / port:       22/tcp
```

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:
Solution type: VendorFix
Upgrade to OpenSSH version 7.6 or later.

Affected Software/OS
OpenSSH versions before 7.6 on Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'sftp-server' Security Bypass Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.812050
Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
cve: CVE-2017-15906
url: https://www.openssh.com/txt/release-7.6
url: http://www.securityfocus.com/bid/101552
url: https://github.com/openbsd/src/commit/a6981567e8e
cert-bund: WID-SEC-2024-1082
cert-bund: CB-K20/0041
cert-bund: CB-K18/0137
cert-bund: CB-K17/2126
cert-bund: CB-K17/2014
cert-bund: CB-K17/2002
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2019-0362
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-2068
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1568
dfn-cert: DFN-CERT-2018-0150
dfn-cert: DFN-CERT-2017-2217
dfn-cert: DFN-CERT-2017-2100
dfn-cert: DFN-CERT-2017-2093
```

[return to 192.168.56.103]

2.1.24 Medium 8181/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2023-05-13 05:33:38.
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Impact

An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.

Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`

OID:1.3.6.1.4.1.25623.1.0.113054

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Summary
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪--------------------------------------------------
TLSv1.0          | 10
TLSv1.1          | 10
TLSv1.2          | 10
```

Impact
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.

Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`

OID:1.3.6.1.4.1.25623.1.0.117761

Version used: `2024-02-02T05:06:11Z`

References

```
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.1
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.1`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

References
```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References
```
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html
```

[return to 192.168.56.103]

2.1.25 Medium 8282/tcp

Medium (CVSS: 6.8)
NVT: Apache Tomcat servlet/JSP container default files

Product detection result
```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary
The Apache Tomcat servlet/JSP container has default files installed.

Vulnerability Detection Result
```
The following default files were found :
http://192.168.56.103:8282/examples/servlets/index.html
http://192.168.56.103:8282/examples/jsp/snp/snoop.jsp
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://192.168.56.103:8282/examples/jsp/index.html
```

Impact

These files should be removed as they may help an attacker to guess the exact version of the Apache Tomcat which is running on this host and may provide other useful information.

Solution:

Solution type: Mitigation

Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.

Vulnerability Insight

Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container.

Vulnerability Detection Method

Details: `Apache Tomcat servlet/JSP container default files`

OID:1.3.6.1.4.1.25623.1.0.12085

Version used: `2023-08-01T13:29:10Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`

Method: `Apache Tomcat Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.107652)

Medium (CVSS: 6.5)

NVT: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to multiple access bypass vulnerabilities.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.50
Installation
path / port:       8282/tcp
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successfully exploiting these issues will allow remote attackers to bypass security constraints to access ostensibly restricted resources on the target system.

Solution:
Solution type: VendorFix
Upgrade to Apache Tomcat version 9.0.5, 8.5.28, 8.0.50, 7.0.85 or later.

Affected Software/OS
Apache Tomcat versions 9.0.0.M1 to 9.0.4
Apache Tomcat versions 8.5.0 to 8.5.27
Apache Tomcat versions 8.0.0.RC1 to 8.0.49
Apache Tomcat versions 7.0.0 to 7.0.84 on Windows.

Vulnerability Insight
Multiple flaws are due to:
- The system does not properly enforce security constraints that defined by annotations of Servlets in certain cases, depending on the order that Servlets are loaded.
- The URL pattern of ” (the empty string) which exactly maps to the context root was not correctly handled when used as part of a security constraint definition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilit.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.812784
Version used: `2024-02-15T05:05:40Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
```
cve: CVE-2018-1305
cve: CVE-2018-1304
url: http://tomcat.apache.org/security-9.html
url: http://www.securityfocus.com/bid/103144
url: http://www.securityfocus.com/bid/103170
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
url: https://lists.apache.org/thread.html/b1d7e2425d6fd2cebed40d318f9365b4454607
↪7e10949b01b1f8a0fb@%3Cannounce.tomcat.apache.org%3E
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K19/1121
cert-bund: CB-K19/0321
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/1007
cert-bund: CB-K18/1006
cert-bund: CB-K18/1005
cert-bund: CB-K18/0790
cert-bund: CB-K18/0420
cert-bund: CB-K18/0349
dfn-cert: DFN-CERT-2019-1627
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-2125
dfn-cert: DFN-CERT-2018-2103
dfn-cert: DFN-CERT-2018-1753
dfn-cert: DFN-CERT-2018-1407
dfn-cert: DFN-CERT-2018-1274
dfn-cert: DFN-CERT-2018-1253
dfn-cert: DFN-CERT-2018-1038
dfn-cert: DFN-CERT-2018-0922
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0455
dfn-cert: DFN-CERT-2018-0378
```

Medium (CVSS: 6.4)
NVT: Apache Axis2 <= 1.6.2 Multiple Vulnerabilities

Summary
Apache Axis2 is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0
Fixed version:     None
Installation
path / port:       /axis2
```

Impact
Successfully exploiting these issues allows attackers to:
- CVE-2012-5785: perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks
- CVE-2012-4418: may allow unauthenticated attackers to construct specially crafted messages that can be successfully verified and contain arbitrary content. This may aid in further attacks
- CVE-2012-5351: allows remote attackers to forge messages and bypass authentication

Solution:
Solution type: WillNotFix

. . . continues on next page . . .

. . . continued from previous page . . .

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

The issue affects versions up to 1.6.2.

Vulnerability Insight

The following flaws exist:

- CVE-2012-5785: a security-bypass vulnerability because the application fails to properly validate SSL certificates from the server
- CVE-2012-4418: a security vulnerability involving XML signature wrapping
- CVE-2012-5351: a SAML assertion that lacks a Signature element, aka a 'Signature exclusion attack'

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Axis2 <= 1.6.2 Multiple Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.111004

Version used: `2023-12-20T05:05:58Z`

References

```
cve: CVE-2012-5785
cve: CVE-2012-4418
cve: CVE-2012-5351
url: https://issues.apache.org/jira/browse/AXIS2C-1607
url: http://www.securityfocus.com/bid/56408
url: http://www.securityfocus.com/bid/55508
```

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following URLs requires Basic Authentication (URL:realm name):
http://192.168.56.103:8282/host-manager/html:"Tomcat Host Manager Application"
http://192.168.56.103:8282/manager/html:"Tomcat Manager Application"
http://192.168.56.103:8282/manager/status:"Tomcat Manager Application"
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References
```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

Medium (CVSS: 4.3)
NVT: Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows

Product detection result
```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary
Apache Tomcat is prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 8.0.33
Fixed version:     8.5.86
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       8282/tcp
```

Solution:
Solution type: VendorFix
Update to version 8.5.86, 9.0.72, 10.1.6, 11.0.0-M3 or later.

Affected Software/OS
Apache Tomcat versions through 8.5.85, 9.0.0-M1 through 9.0.71, 10.x through 10.1.5 and 11.0.0-M1 through 11.0.0-M2.

Vulnerability Insight
When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Tomcat did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows`
OID:1.3.6.1.4.1.25623.1.0.104654
Version used: `2024-06-07T05:05:42Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
```
cve: CVE-2023-28708
url: https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67
url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3
url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.6
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.72
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.86
cert-bund: WID-SEC-2024-1238
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2023-2674
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1808
cert-bund: WID-SEC-2023-1784
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1782
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1021
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1017
cert-bund: WID-SEC-2023-0717
dfn-cert: DFN-CERT-2023-2778
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2054
dfn-cert: DFN-CERT-2023-0772
dfn-cert: DFN-CERT-2023-0763
dfn-cert: DFN-CERT-2023-0640
```

Medium (CVSS: 4.3)
NVT: Apache Tomcat Open Redirect Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

When the default servlet in Apache Tomcat returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice.

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.5.34
Installation
path / port:       8282/tcp
```

Solution:

Solution type: VendorFix

Update to version 7.0.91, 8.5.34, 9.0.12 or later.

Affected Software/OS

Apache Tomcat 9.0.0.M1-9.0.11, 8.5.0-8.5.33, 7.0.23-7.0.90 and probably 8.0.x.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache Tomcat Open Redirect Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.141569

Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:apache:tomcat:8.0.33`

Method: `Apache Tomcat Detection Consolidation`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2018-11784
url: http://tomcat.apache.org/security-9.html
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2023-0531
cert-bund: WID-SEC-2023-0460
cert-bund: CB-K20/0029
cert-bund: CB-K19/1121
cert-bund: CB-K19/0907
cert-bund: CB-K19/0616
cert-bund: CB-K19/0320
cert-bund: CB-K19/0050
cert-bund: CB-K18/0963
dfn-cert: DFN-CERT-2019-2710
dfn-cert: DFN-CERT-2019-2159
dfn-cert: DFN-CERT-2019-1562
dfn-cert: DFN-CERT-2019-1237
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0147
dfn-cert: DFN-CERT-2019-0104
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-2000
```

[return to 192.168.56.103]

2.1.26 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary

The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
```

[return to 192.168.56.103]

2.1.27 Low general/tcp

Low (CVSS: 3.7)
NVT: Oracle Java SE Security Updates - 02 - (cpujul2020) - Windows

Summary
Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful attacks of these vulnerabilities can result in unauthorized ability to cause a partial denial of service.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 7u261 (1.7.0.261) and earlier, 8u251 (1.8.0.251) and earlier on Windows.

Vulnerability Insight

The flaws exist due to errors in the 'Libraries' component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Updates - 02 - (cpujul2020) - Windows`

OID:1.3.6.1.4.1.25623.1.0.118164

Version used: `2024-02-26T14:36:40Z`

References

```
cve: CVE-2020-14578
cve: CVE-2020-14579
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1522
cert-bund: WID-SEC-2022-1285
cert-bund: CB-K20/1075
cert-bund: CB-K20/0715
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-1762
dfn-cert: DFN-CERT-2020-1531
```

Low (CVSS: 3.7)

NVT: Oracle Java SE Security Update (jan2023) 03 - Windows

Summary

Oracle Java SE is prone to an input validation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attacker to manipulate data.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u351 and earlier, 11.0.17, 17.0.5, 19.0.1 and earlier on Windows.

Vulnerability Insight

The flaw is due to an improper input validation within the Sound component in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jan2023) 03 - Windows`

OID:1.3.6.1.4.1.25623.1.0.826783

Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-21843
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0128
dfn-cert: DFN-CERT-2023-1174
dfn-cert: DFN-CERT-2023-1139
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0717
dfn-cert: DFN-CERT-2023-0605
dfn-cert: DFN-CERT-2023-0256
dfn-cert: DFN-CERT-2023-0217
dfn-cert: DFN-CERT-2023-0125
dfn-cert: DFN-CERT-2023-0124
```

Low (CVSS: 3.7)

NVT: Oracle Java SE Security Update (jul2023) 04 - Windows

Summary

Oracle Java SE is prone to remote code execution (RCE) vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u371 and earlier, 11.0.19, 20.0.1 and earlier on Windows.

Vulnerability Insight

The flaw is due to improper application of hotspot module within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2023) 04 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832319

Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-22044
url: https://www.oracle.com/security-alerts/cpujul2023.html
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1972
dfn-cert: DFN-CERT-2023-1657
dfn-cert: DFN-CERT-2023-1653
```

Low (CVSS: 3.7)

NVT: Oracle Java SE Security Update (jul2023) 04 - Windows

Summary

Oracle Java SE is prone to remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u371 and earlier, 11.0.19, 20.0.1 and earlier on Windows.

Vulnerability Insight

The flaw is due to improper application of hotspot module within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2023) 04 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832319

Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-22044
url: https://www.oracle.com/security-alerts/cpujul2023.html
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1972
dfn-cert: DFN-CERT-2023-1657
dfn-cert: DFN-CERT-2023-1653
```

Low (CVSS: 3.7)

NVT: Oracle Java SE Security Update (jul2023) 05 - Windows

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u371 and earlier, 11.0.19, 17.0.7, 20.0.1 and earlier on Windows.

Vulnerability Insight

The flaw is due to improper application of hotspot module and libraries within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2023) 05 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832322

Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-22045
cve: CVE-2023-22049
url: https://www.oracle.com/security-alerts/cpujul2023.html
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1814
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-3167
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-2042
dfn-cert: DFN-CERT-2023-2031
dfn-cert: DFN-CERT-2023-1990
dfn-cert: DFN-CERT-2023-1972
dfn-cert: DFN-CERT-2023-1935
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1657
dfn-cert: DFN-CERT-2023-1653
```

Low (CVSS: 3.7)
NVT: Oracle Java SE Security Update (jul2023) 05 - Windows

Summary

Oracle Java SE is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation will allow remote attacker to manipulate data and execute arbitrary code.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 8u371 and earlier, 11.0.19, 17.0.7, 20.0.1 and earlier on Windows.

Vulnerability Insight

The flaw is due to improper application of hotspot module and libraries within the Java SE engine component in Oracle Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (jul2023) 05 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832322

Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-22045
cve: CVE-2023-22049
url: https://www.oracle.com/security-alerts/cpujul2023.html
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1814
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-3167
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-2042
dfn-cert: DFN-CERT-2023-2031
dfn-cert: DFN-CERT-2023-1990
dfn-cert: DFN-CERT-2023-1972
dfn-cert: DFN-CERT-2023-1935
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1657
dfn-cert: DFN-CERT-2023-1653
```

Low (CVSS: 3.7)
NVT: Oracle Java SE Security Update (Apr 2024) -01 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation allows an attacker to compromise Oracle Java SE, which can result in unauthorized update, insert or delete access to some of Oracle Java SE.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u401 and prior, 17.0.x through 17.0.10, 11.0.x through 11.0.22, 21.0.x through 21.0.2 and 22.0 on Windows.

Vulnerability Insight
These vulnerabilities exist:
- CVE-2024-21011: An error in the Hotspot component of Oracle Java SE.
- CVE-2024-21094: An error in the Hotspot component of Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (Apr 2024) -01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832952
Version used: `2024-04-25T05:05:14Z`

References

```
cve: CVE-2024-21011
cve: CVE-2024-21094
url: https://www.oracle.com/security-alerts/cpuapr2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0895
dfn-cert: DFN-CERT-2024-1436
dfn-cert: DFN-CERT-2024-1272
dfn-cert: DFN-CERT-2024-1251
dfn-cert: DFN-CERT-2024-1032
dfn-cert: DFN-CERT-2024-1005
```

. . . continues on next page . . .

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2024-1004

Low (CVSS: 3.7)
NVT: Oracle Java SE Security Update (jan2023) 03 - Windows

Summary
Oracle Java SE is prone to an input validation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch from vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to manipulate data.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u351 and earlier, 11.0.17, 17.0.5, 19.0.1 and earlier on Windows.

Vulnerability Insight
The flaw is due to an improper input validation within the Sound component in Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2023) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.826783
Version used: `2023-10-13T05:06:10Z`

References

```
cve: CVE-2023-21843
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixJAVA
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0128
dfn-cert: DFN-CERT-2023-1174
dfn-cert: DFN-CERT-2023-1139
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0717
dfn-cert: DFN-CERT-2023-0605
dfn-cert: DFN-CERT-2023-0256
dfn-cert: DFN-CERT-2023-0217
dfn-cert: DFN-CERT-2023-0125
dfn-cert: DFN-CERT-2023-0124
```

Low (CVSS: 3.7)
NVT: Oracle Java SE Security Update (Apr 2024) -01 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation allows an attacker to compromise Oracle Java SE, which can result in unauthorized update, insert or delete access to some of Oracle Java SE.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u401 and prior, 17.0.x through 17.0.10, 11.0.x through 11.0.22, 21.0.x through 21.0.2 and 22.0 on Windows.

Vulnerability Insight
These vulnerabilities exist:
- CVE-2024-21011: An error in the Hotspot component of Oracle Java SE.
- CVE-2024-21094: An error in the Hotspot component of Oracle Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (Apr 2024) -01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832952
Version used: `2024-04-25T05:05:14Z`

References

```
cve: CVE-2024-21011
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2024-21094
url: https://www.oracle.com/security-alerts/cpuapr2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0895
dfn-cert: DFN-CERT-2024-1436
dfn-cert: DFN-CERT-2024-1272
dfn-cert: DFN-CERT-2024-1251
dfn-cert: DFN-CERT-2024-1032
dfn-cert: DFN-CERT-2024-1005
dfn-cert: DFN-CERT-2024-1004
```

Low (CVSS: 3.7)
NVT: Oracle Java SE Security Updates - 02 - (cpujul2020) - Windows

Summary
Oracle Java SE is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful attacks of these vulnerabilities can result in unauthorized ability to cause a partial denial of service.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 7u261 (1.7.0.261) and earlier, 8u251 (1.8.0.251) and earlier on Windows.

Vulnerability Insight
The flaws exist due to errors in the 'Libraries' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates - 02 - (cpujul2020) - Windows`
OID:1.3.6.1.4.1.25623.1.0.118164
Version used: `2024-02-26T14:36:40Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-14578
cve: CVE-2020-14579
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA
cert-bund: WID-SEC-2023-0016
cert-bund: WID-SEC-2022-1522
cert-bund: WID-SEC-2022-1285
cert-bund: CB-K20/1075
cert-bund: CB-K20/0715
dfn-cert: DFN-CERT-2020-2571
dfn-cert: DFN-CERT-2020-1762
dfn-cert: DFN-CERT-2020-1531
```

Low (CVSS: 3.3)
NVT: Microsoft Windows NETLOGON Privilege Elevation Vulnerability (3068457)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-071.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote man-in-the-middle attacker to conduct SMB relay attacks on domain environments utilizing SMB Signing enforcement, and decrypt SMB3 communications intercepted.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows Server 2012/R2
- Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Flaw is due to Netlogon service improperly establishes a secure communications channel belonging to a different machine with a spoofed computer name.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows NETLOGON Privilege Elevation Vulnerability (3068457)`
OID:1.3.6.1.4.1.25623.1.0.805075
Version used: `2023-07-25T05:05:58Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2015-2374
url: https://support.microsoft.com/en-us/kb/3068457
url: http://www.securityfocus.com/bid/75633
url: https://technet.microsoft.com/en-us/library/security/MS15-071
cert-bund: CB-K15/1013
dfn-cert: DFN-CERT-2015-1060
```

Low (CVSS: 3.3)
NVT: Microsoft .NET Framework DoS Vulnerability (KB5013870)

Summary

This host is missing an important security update according to Microsoft KB5013870

Vulnerability Detection Result

```
Vulnerable range:  2.0.50727 - 2.0.50727.8963
File checked:      C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.dll
File version:      2.0.50727.5420
```

Impact

Successful exploitation will allow an attacker to cause a denial of service condition.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Microsoft .NET Framework 3.5.1, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 R2 SP1.

Vulnerability Insight

The flaw exists due to an error in .NET Framework which allows a local attacker to cause a denial of service on an affected system.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft .NET Framework DoS Vulnerability (KB5013870)`

OID:1.3.6.1.4.1.25623.1.0.821227

Version used: `2023-06-08T05:05:11Z`

References

```
cve: CVE-2022-30130
url: https://support.microsoft.com/en-us/help/5013870
cert-bund: WID-SEC-2022-1251
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0539
cert-bund: CB-K22/0588
dfn-cert: DFN-CERT-2022-1039
```

Low (CVSS: 3.3)
NVT: Microsoft Windows Group Policy Security Feature Bypass Vulnerability (3004361)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-014.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation could allow remote attackers to modify domain controller responses to client requests and revert the Group Policy settings on a system back to default.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
The flaw is due to an error in the Group Policy application of Security Configuration policies.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Group Policy Security Feature Bypass Vulnerability (3004361)`
OID:1.3.6.1.4.1.25623.1.0.805273
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0009
url: https://support.microsoft.com/kb/3004361
url: http://www.securityfocus.com/bid/72476
url: https://technet.microsoft.com/library/security/MS15-014
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://blogs.technet.com/b/srd/archive/2015/02/10/ms15-011-amp-ms15-014-har
↪dening-group-policy.aspx
cert-bund: CB-K15/0171
dfn-cert: DFN-CERT-2015-0175
```

Low (CVSS: 3.1)
NVT: Oracle Java SE Security Update (oct2021) 05 - Windows

Summary
Oracle Java SE is prone to a denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u301 (1.8.0.301) and earlier, 7u311 (1.7.0.311) and earlier on Windows.

Vulnerability Insight
The flaw is due to an error in 'Hotspot' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2021) 05 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818831
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-35588
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0196
cert-bund: CB-K21/1082
dfn-cert: DFN-CERT-2022-1571
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-0366
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
```

Low (CVSS: 3.1)
NVT: Oracle Java SE Security Update (oct2021) 05 - Windows

Summary
Oracle Java SE is prone to a denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply the patch
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to have an impact on availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u301 (1.8.0.301) and earlier, 7u311 (1.7.0.311) and earlier on Windows.

Vulnerability Insight
The flaw is due to an error in 'Hotspot' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (oct2021) 05 - Windows`
OID:1.3.6.1.4.1.25623.1.0.818831
Version used: `2023-04-03T10:19:50Z`

References

```
cve: CVE-2021-35588
url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0196
cert-bund: CB-K21/1082
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-0366
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
```

Low (CVSS: 3.1)
NVT: Microsoft Windows DirectShow Information Disclosure Vulnerability (4010318)

Summary
This host is missing an important security update according to Microsoft Bulletin MS17-021.

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Quartz.dll
File version:     6.6.7601.18741
Vulnerable range: Less than 6.6.7601.23643
```

Impact
Successful exploitation will allow an attacker to obtain information to further compromise a target system.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012/2012R2
- Microsoft Windows 10 Version 1511 x32/x64
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2016

Vulnerability Insight
The flaw exists when windows DirectShow handles objects in memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows DirectShow Information Disclosure Vulnerability (4010318)`
OID:1.3.6.1.4.1.25623.1.0.810596
Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2017-0042
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://support.microsoft.com/en-us/kb/4010318
url: http://www.securityfocus.com/bid/96098
url: https://technet.microsoft.com/library/security/MS17-021
cert-bund: CB-K17/0443
dfn-cert: DFN-CERT-2017-0451
```

Low (CVSS: 3.1)
NVT: Oracle Java SE Security Update (jan2024) 04 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to compromise Oracle Java SE, which can result in unauthorized update, insert or delete access to some of Oracle Java SE.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u391 and earlier on Windows.

Vulnerability Insight
Multiple flaws exist due to multiple errors in the multiple components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2024) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832790
Version used: `2024-02-19T05:05:57Z`

References

```
cve: CVE-2024-20923
cve: CVE-2024-20925
cve: CVE-2024-20922
url: https://www.oracle.com/security-alerts/cpujan2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-0121
dfn-cert: DFN-CERT-2024-0129
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-0128
```

Low (CVSS: 3.1)
NVT: Oracle Java SE Security Update (jan2024) 04 - Windows

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact
Successful exploitation will allow remote attacker to compromise Oracle Java SE, which can result in unauthorized update, insert or delete access to some of Oracle Java SE.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 8u391 and earlier on Windows.

Vulnerability Insight
Multiple flaws exist due to multiple errors in the multiple components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (jan2024) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.832790
Version used: `2024-02-19T05:05:57Z`

References

```
cve: CVE-2024-20923
cve: CVE-2024-20925
cve: CVE-2024-20922
url: https://www.oracle.com/security-alerts/cpujan2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-0121
dfn-cert: DFN-CERT-2024-0129
dfn-cert: DFN-CERT-2024-0128
```

Low (CVSS: 2.6)
NVT: Microsoft Windows .NET Framework Information Disclosure Vulnerability (3048010)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-041.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to view parts of a web configuration file, which could expose sensitive information.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 4
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 2.0
- Microsoft .NET Framework 1.1
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.5, 4.5.1, and 4.5.2

Vulnerability Insight
The flaw exists when ASP.NET improperly handles certain requests on systems that have custom error messages disabled.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows .NET Framework Information Disclosure Vulnerability (3048010)`
OID:1.3.6.1.4.1.25623.1.0.805060
Version used: `2023-07-25T05:05:58Z`

References
```
cve: CVE-2015-1648
url: https://support.microsoft.com/en-us/kb/3048010
url: https://technet.microsoft.com/library/security/MS15-041
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545
```

Low (CVSS: 2.6)
NVT: Oracle Java SE Security Update (Apr 2024) -03 - Windows

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE is prone to a denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files\Java\jre1.8.0_251
```

Impact

Successful exploitation allows an attacker to cause a partial denial of service (partial DOS)

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE 8u401 and prior and 11.0.x through 11.0.22 on Windows.

Vulnerability Insight

The flaw exists due to a NativeUnpack class did not properly validate the memory size when allocating a buffer.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (Apr 2024) -03 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832955

Version used: `2024-04-25T05:05:14Z`

References

```
cve: CVE-2024-21085
url: https://www.oracle.com/security-alerts/cpuapr2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0895
dfn-cert: DFN-CERT-2024-1436
dfn-cert: DFN-CERT-2024-1251
dfn-cert: DFN-CERT-2024-1032
dfn-cert: DFN-CERT-2024-1005
dfn-cert: DFN-CERT-2024-1004
```

Low (CVSS: 2.6)

NVT: Oracle Java SE Security Update (Apr 2024) -03 - Windows

Summary

Oracle Java SE is prone to a denial of service vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.0update_251
Fixed version:     Apply patch provided by the vendor
Installation
path / port:       C:\Program Files (x86)\Java\jre1.8.0_251
```

Impact

Successful exploitation allows an attacker to cause a partial denial of service (partial DOS)

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE 8u401 and prior and 11.0.x through 11.0.22 on Windows.

Vulnerability Insight

The flaw exists due to a NativeUnpack class did not properly validate the memory size when allocating a buffer.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Update (Apr 2024) -03 - Windows`

OID:1.3.6.1.4.1.25623.1.0.832955

Version used: `2024-04-25T05:05:14Z`

References

```
cve: CVE-2024-21085
url: https://www.oracle.com/security-alerts/cpuapr2024.html#AppendixJAVA
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0895
dfn-cert: DFN-CERT-2024-1436
dfn-cert: DFN-CERT-2024-1251
dfn-cert: DFN-CERT-2024-1032
dfn-cert: DFN-CERT-2024-1005
dfn-cert: DFN-CERT-2024-1004
```

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 719532
Packet 2: 719638
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

Low (CVSS: 2.1)
NVT: Microsoft Windows Task Scheduler security Feature Bypass Vulnerability (3030377)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-028.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
File checked:     C:\Windows\Ubpm.dll
File version:     6.1.7600.16385
Vulnerable range:
```

Impact

Successful exploitation will allow local attacker to gain elevated privileges.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012/R2

Vulnerability Insight

Flaw exists as Windows Task Scheduler fails to properly validate and enforce impersonation levels.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Task Scheduler security Feature Bypass Vulnerability (3030377)`

OID:1.3.6.1.4.1.25623.1.0.805144

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-0084
url: https://support.microsoft.com/kb/3030377
url: https://technet.microsoft.com/library/security/MS15-028
cert-bund: CB-K15/0319
dfn-cert: DFN-CERT-2015-0324
```

Low (CVSS: 2.1)
NVT: Microsoft Windows Kernel-Mode Driver Privilege Elevation Vulnerability (3045171)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-051.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

... continues on next page ...

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to gain access to kernel memory contents that contain sensitive information about the system.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows Server 2012/R2
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows 2003 x32/x64 Service Pack 2 and prior
- Microsoft Windows Vista x32/x64 Service Pack 2 and prior
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior
- Microsoft Windows Server 2008 R2 x64 Service Pack 1 and prior

Vulnerability Insight

The flaw is due to the kernel-mode driver leaking private address information during a function call

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Kernel-Mode Driver Privilege Elevation Vulnerability (3045171)`

OID:1.3.6.1.4.1.25623.1.0.805381

Version used: `2023-07-25T05:05:58Z`

References

```
cve: CVE-2015-1676
cve: CVE-2015-1677
cve: CVE-2015-1678
cve: CVE-2015-1679
cve: CVE-2015-1680
url: https://support.microsoft.com/kb/3045171
url: http://www.securityfocus.com/bid/74483
url: http://www.securityfocus.com/bid/74494
url: http://www.securityfocus.com/bid/74495
url: http://www.securityfocus.com/bid/74496
url: http://www.securityfocus.com/bid/74497
url: https://technet.microsoft.com/library/security/MS15-051
cert-bund: CB-K15/0668
dfn-cert: DFN-CERT-2015-0689
```

[return to 192.168.56.103]

2.1.28 Low 9200/tcp

Low (CVSS: 3.1)
NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     6.8.13
Installation
path / port:       /
```

Impact
This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.

Solution:
Solution type: VendorFix
Update to version 6.8.13, 7.9.2 or later.

Affected Software/OS
Elasticsearch versions before 6.8.13 and 7.x before 7.9.2.

Vulnerability Insight
A document disclosure flaw was found in Elasticsearch when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)`
OID:1.3.6.1.4.1.25623.1.0.117181
Version used: `2021-08-17T12:00:57Z`

References

```
cve: CVE-2020-7020
url: https://discuss.elastic.co/t/elastic-stack-7-9-3-and-6-8-13-security-update
↪/253033
url: https://www.elastic.co/community/security
cert-bund: WID-SEC-2022-0607
dfn-cert: DFN-CERT-2022-1530
```

[return to 192.168.56.103]

2.1.29 Low 3306/tcp

Low (CVSS: 3.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpujul2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.

Vulnerability Insight
An unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Connection' sub-component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.808593
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-5444
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91987
advisory-id: cpujul2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
```

Low (CVSS: 3.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.10 Security Update (cpujul2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.10.

Vulnerability Insight

An unspecified error exists in the 'MySQL Server' component via unknown vectors related to the 'Security Encryption' sub-component.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.10 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.808594
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-3452
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91999
advisory-id: cpujul2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
```

Low (CVSS: 3.5)
NVT: Oracle MySQL Unspecified Vulnerability-04 (Jul 2015)

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to cause denial of service attack.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on Windows.

Vulnerability Insight
Unspecified error exists in the MySQL Server component via unknown vectors related to Server : Optimizer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Unspecified Vulnerability-04 (Jul 2015)`
OID:1.3.6.1.4.1.25623.1.0.805931
Version used: `2024-02-20T05:05:48Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-4757
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75759
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1020
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071
```

Low (CVSS: 3.5)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-07 (Oct 2015) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect integrity via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on windows

Vulnerability Insight
Unspecified error exists in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-07 (Oct 2015) - Windows`
OID:1.3.6.1.4.1.25623.1.0.805770
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2015-4864
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77187
cert-bund: CB-K16/0245
cert-bund: CB-K15/1844
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1638
```

Low (CVSS: 3.5)
NVT: Oracle MySQL Server Multiple Vulnerabilities - 05 - (Nov 2012) - Windows

Product detection result

... continues on next page ...

. . . continued from previous page . . .

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow an attacker to disclose potentially sensitive information and manipulate certain data.

Solution:
Solution type: VendorFix
Apply the patch from the linked references or upgrade to latest version.

Affected Software/OS
Oracle MySQL version 5.5.x to 5.5.25 on Windows.

Vulnerability Insight
The flaw is due to unspecified error in MySQL server component vectors server.

Vulnerability Detection Method
Details: `Oracle MySQL Server Multiple Vulnerabilities - 05 - (Nov 2012) - Windows`
OID:1.3.6.1.4.1.25623.1.0.803115
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2012-3156
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56013
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
```

Low (CVSS: 2.8)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 06 (Jan 2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Replication.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 06 (Jan 2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.804077
Version used: `2024-02-09T05:06:25Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2014-0420
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64888
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/0187
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
```

Low (CVSS: 2.7)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.45
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.6.45, 5.7.19 or later.

Affected Software/OS

Oracle MySQL Server versions 5.6.44 and prior and 5.7 through 5.7.18.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Wi.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.142643

Version used: `2021-09-07T14:01:38Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2019-2730
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL
advisory-id: cpujul2019
cert-bund: CB-K19/0620
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-1453
```

Low (CVSS: 2.7)
NVT: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.41
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.7.41, 8.0.32 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.40 and prior and 8.x through 8.0.31.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpuapr2023) - Win.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.149532
Version used: `2023-10-13T05:06:10Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2023-21963
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-1033
dfn-cert: DFN-CERT-2023-0885
```

Low (CVSS: 1.5)
NVT: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.31
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow local users to affect availability.

Solution:
Solution type: VendorFix
Update to version 5.5.31, 5.6.10 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.9.

Vulnerability Insight
An unspecified error exists in the MySQL Server component via unknown vectors related to Server Partition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) -.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809813
Version used: `2022-04-25T14:50:49Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-1502
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59239
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0798
```

[return to 192.168.56.103]

2.1.30 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

References

`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 192.168.56.103]