Scan Report

June 28, 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 "Metasploitable_CW". The scan started at Thu Jun 27 11:21:56 2024 UTC and ended at . 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
192.168.56.105	82	50	3	0	0
Total: 1	82	50	3	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 135 results selected by the filtering described above. Before filtering there were 926 results.

2 Results per Host

2.1 192.168.56.105

Host scan start	Thu Jun 27 11:22:32 2024 UTC
Host scan end	

Service (Port)	Threat Level
631/tcp	High
21/tcp	High
22/tcp	High
general/tcp	High
631/tcp	Medium
80/tcp	Medium
21/tcp	Medium
22/tcp	Medium
general/tcp	Medium
general/icmp	Low
22/tcp	Low
general/tcp	Low

2.1.1 High 631/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

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_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
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`

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
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 192.168.56.105]

2.1.2 High 21/tcp

High (CVSS: 10.0)
NVT: ProFTPD ‘mod_copy‘ Unauthenticated Copying Of Files Via SITE CPFR/CPTO

Summary
ProFTPD is prone to an unauthenticated copying of files vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

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

Impact

Under some circumstances this could result in remote code execution

Solution:

Solution type: VendorFix

Ask the vendor for an update

Vulnerability Detection Method

Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO

Details: `ProFTPD ‘mod_copy‘ Unauthenticated Copying Of Files Via SITE CPFR/CPTO`

OID:1.3.6.1.4.1.25623.1.0.105254

Version used: `2022-12-02T10:11:16Z`

References

```
cve: CVE-2015-3306
url: http://bugs.proftpd.org/show_bug.cgi?id=4169
cert-bund: CB-K15/0791
cert-bund: CB-K15/0553
dfn-cert: DFN-CERT-2015-0839
dfn-cert: DFN-CERT-2015-0576
```

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>
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

. . . continues on next page . . .

. . . continued from previous page . . .

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 192.168.56.105]

2.1.3 High 22/tcp

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

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
```

[return to 192.168.56.105]

2.1.4 High general/tcp

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Jul 2014) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or possibly other impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle Java SE 6 update 75 and prior, 7 update 60 and prior, and 8 update 5.0 and prior on Linux.

Vulnerability Insight
Multiple flaws exist:
- Two unspecified errors related to the Deployment subcomponent.
- An unspecified error in the Hotspot subcomponent related to bytecode verification.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Jul 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108416
Version used: `2024-02-20T14:37:13Z`

References
```
cve: CVE-2014-4265
cve: CVE-2014-4219
cve: CVE-2014-4227
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68603
url: http://www.securityfocus.com/bid/68620
url: http://www.securityfocus.com/bid/68632
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2014) - Linux

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation will allow attackers to perform certain actions with escalated privileges, disclose sensitive information and compromise a user's system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- Multiple errors related to the Deployment subcomponent.
- An XXE (Xml eXternal Entity) injection error in com/sun/org/apache/xerces/internal/impl/XMLEntityManager.j script.
- An error in windows/native/sun/awt/splashscreen/splashscreen_sys.c script related to handling of splash images.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2014) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108414

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-6532
cve: CVE-2014-6517
cve: CVE-2014-6515
cve: CVE-2014-6513
cve: CVE-2014-6503
cve: CVE-2014-6493
cve: CVE-2014-6492
cve: CVE-2014-6466
cve: CVE-2014-6458
cve: CVE-2014-4288
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70456
url: http://www.securityfocus.com/bid/70460
url: http://www.securityfocus.com/bid/70468
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/70470
url: http://www.securityfocus.com/bid/70484
url: http://www.securityfocus.com/bid/70507
url: http://www.securityfocus.com/bid/70518
url: http://www.securityfocus.com/bid/70552
url: http://www.securityfocus.com/bid/70565
url: http://www.securityfocus.com/bid/70569
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2014) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow attackers to perform certain actions with escalated privileges, disclose sensitive information and compromise a user's system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors related to the Deployment subcomponent.
- An XXE (Xml eXternal Entity) injection error in com/sun/org/apache/xerces/internal/impl/XMLEntityManager.j script.
- An error in windows/native/sun/awt/splashscreen/splashscreen_sys.c script related to handling of splash images.

. . . 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 JRE Multiple Unspecified Vulnerabilities-02 (Oct 2014) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108414

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-6532
cve: CVE-2014-6517
cve: CVE-2014-6515
cve: CVE-2014-6513
cve: CVE-2014-6503
cve: CVE-2014-6493
cve: CVE-2014-6492
cve: CVE-2014-6466
cve: CVE-2014-6458
cve: CVE-2014-4288
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70456
url: http://www.securityfocus.com/bid/70460
url: http://www.securityfocus.com/bid/70468
url: http://www.securityfocus.com/bid/70470
url: http://www.securityfocus.com/bid/70484
url: http://www.securityfocus.com/bid/70507
url: http://www.securityfocus.com/bid/70518
url: http://www.securityfocus.com/bid/70552
url: http://www.securityfocus.com/bid/70565
url: http://www.securityfocus.com/bid/70569
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2015) - Linux

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via different vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 101 and prior, 7 update 85 and prior, 8 update 60 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108399
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-4902
cve: CVE-2015-4903
cve: CVE-2015-4911
cve: CVE-2015-4893
cve: CVE-2015-4883
cve: CVE-2015-4882
cve: CVE-2015-4881
cve: CVE-2015-4872
cve: CVE-2015-4860
cve: CVE-2015-4844
cve: CVE-2015-4843
cve: CVE-2015-4842
cve: CVE-2015-4835
cve: CVE-2015-4806
cve: CVE-2015-4805
cve: CVE-2015-4803
cve: CVE-2015-4734
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
url: http://www.securityfocus.com/bid/77241
url: http://www.securityfocus.com/bid/77194
url: http://www.securityfocus.com/bid/77209
url: http://www.securityfocus.com/bid/77207
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/77161
url: http://www.securityfocus.com/bid/77181
url: http://www.securityfocus.com/bid/77159
url: http://www.securityfocus.com/bid/77211
url: http://www.securityfocus.com/bid/77162
url: http://www.securityfocus.com/bid/77164
url: http://www.securityfocus.com/bid/77160
url: http://www.securityfocus.com/bid/77154
url: http://www.securityfocus.com/bid/77148
url: http://www.securityfocus.com/bid/77126
url: http://www.securityfocus.com/bid/77163
url: http://www.securityfocus.com/bid/77200
url: http://www.securityfocus.com/bid/77192
cert-bund: CB-K16/1842
cert-bund: CB-K16/1080
cert-bund: CB-K15/1759
cert-bund: CB-K15/1751
cert-bund: CB-K15/1713
cert-bund: CB-K15/1555
cert-bund: CB-K15/1552
dfn-cert: DFN-CERT-2015-1860
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1812
dfn-cert: DFN-CERT-2015-1641
dfn-cert: DFN-CERT-2015-1633
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via different vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE 6 update 101 and prior, 7 update 85 and prior, 8 update 60 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2015) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108399

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-4902
cve: CVE-2015-4903
cve: CVE-2015-4911
cve: CVE-2015-4893
cve: CVE-2015-4883
cve: CVE-2015-4882
cve: CVE-2015-4881
cve: CVE-2015-4872
cve: CVE-2015-4860
cve: CVE-2015-4844
cve: CVE-2015-4843
cve: CVE-2015-4842
cve: CVE-2015-4835
cve: CVE-2015-4806
cve: CVE-2015-4805
cve: CVE-2015-4803
cve: CVE-2015-4734
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
url: http://www.securityfocus.com/bid/77241
url: http://www.securityfocus.com/bid/77194
url: http://www.securityfocus.com/bid/77209
url: http://www.securityfocus.com/bid/77207
url: http://www.securityfocus.com/bid/77161
url: http://www.securityfocus.com/bid/77181
url: http://www.securityfocus.com/bid/77159
url: http://www.securityfocus.com/bid/77211
url: http://www.securityfocus.com/bid/77162
url: http://www.securityfocus.com/bid/77164
url: http://www.securityfocus.com/bid/77160
url: http://www.securityfocus.com/bid/77154
url: http://www.securityfocus.com/bid/77148
url: http://www.securityfocus.com/bid/77126
url: http://www.securityfocus.com/bid/77163
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/77200
url: http://www.securityfocus.com/bid/77192
cert-bund: CB-K16/1842
cert-bund: CB-K16/1080
cert-bund: CB-K15/1759
cert-bund: CB-K15/1751
cert-bund: CB-K15/1713
cert-bund: CB-K15/1555
cert-bund: CB-K15/1552
dfn-cert: DFN-CERT-2015-1860
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1812
dfn-cert: DFN-CERT-2015-1641
dfn-cert: DFN-CERT-2015-1633
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via different vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 101 and prior, 7 update 85 and prior, 8 update 60 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108399
Version used: `2024-02-20T14:37:13Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2015-4902
cve: CVE-2015-4903
cve: CVE-2015-4911
cve: CVE-2015-4893
cve: CVE-2015-4883
cve: CVE-2015-4882
cve: CVE-2015-4881
cve: CVE-2015-4872
cve: CVE-2015-4860
cve: CVE-2015-4844
cve: CVE-2015-4843
cve: CVE-2015-4842
cve: CVE-2015-4835
cve: CVE-2015-4806
cve: CVE-2015-4805
cve: CVE-2015-4803
cve: CVE-2015-4734
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
url: http://www.securityfocus.com/bid/77241
url: http://www.securityfocus.com/bid/77194
url: http://www.securityfocus.com/bid/77209
url: http://www.securityfocus.com/bid/77207
url: http://www.securityfocus.com/bid/77161
url: http://www.securityfocus.com/bid/77181
url: http://www.securityfocus.com/bid/77159
url: http://www.securityfocus.com/bid/77211
url: http://www.securityfocus.com/bid/77162
url: http://www.securityfocus.com/bid/77164
url: http://www.securityfocus.com/bid/77160
url: http://www.securityfocus.com/bid/77154
url: http://www.securityfocus.com/bid/77148
url: http://www.securityfocus.com/bid/77126
url: http://www.securityfocus.com/bid/77163
url: http://www.securityfocus.com/bid/77200
url: http://www.securityfocus.com/bid/77192
cert-bund: CB-K16/1842
cert-bund: CB-K16/1080
cert-bund: CB-K15/1759
cert-bund: CB-K15/1751
cert-bund: CB-K15/1713
cert-bund: CB-K15/1555
cert-bund: CB-K15/1552
dfn-cert: DFN-CERT-2015-1860
dfn-cert: DFN-CERT-2015-1853
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-1812
dfn-cert: DFN-CERT-2015-1641
dfn-cert: DFN-CERT-2015-1633
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Feb 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to gain escalated privileges, conduct a denial of service attack, bypass sandbox restrictions and execute arbitrary code.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist due to:
- An unspecified error in the JAX-WS component related to insufficient privilege checks.
- Two unspecified errors in the Deployment component.
- An unspecified error in the 'Libraries' component.
- An error in vm/classfile/verifier.cpp script related to insufficient verification of invokespecial calls.
- A NULL pointer dereference error in the MulticastSocket implementation.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Feb 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108401
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0412
cve: CVE-2015-0406
cve: CVE-2015-0403
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-0400
cve: CVE-2014-6601
cve: CVE-2014-6587
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72136
url: http://www.securityfocus.com/bid/72154
url: http://www.securityfocus.com/bid/72148
url: http://www.securityfocus.com/bid/72159
url: http://www.securityfocus.com/bid/72132
url: http://www.securityfocus.com/bid/72168
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0308
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Feb 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to gain escalated privileges, conduct a denial of service attack, bypass sandbox restrictions and execute arbitrary code.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Oracle Java SE 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist due to:
- An unspecified error in the JAX-WS component related to insufficient privilege checks.
- Two unspecified errors in the Deployment component.
- An unspecified error in the 'Libraries' component.
- An error in vm/classfile/verifier.cpp script related to insufficient verification of invokespecial calls.
- A NULL pointer dereference error in the MulticastSocket implementation.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Feb 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108401
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0412
cve: CVE-2015-0406
cve: CVE-2015-0403
cve: CVE-2015-0400
cve: CVE-2014-6601
cve: CVE-2014-6587
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72136
url: http://www.securityfocus.com/bid/72154
url: http://www.securityfocus.com/bid/72148
url: http://www.securityfocus.com/bid/72159
url: http://www.securityfocus.com/bid/72132
url: http://www.securityfocus.com/bid/72168
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0308
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Feb 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to gain escalated privileges, conduct a denial of service attack, bypass sandbox restrictions and execute arbitrary code.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist due to:
- An unspecified error in the JAX-WS component related to insufficient privilege checks.
- Two unspecified errors in the Deployment component.
- An unspecified error in the 'Libraries' component.
- An error in vm/classfile/verifier.cpp script related to insufficient verification of invokespecial calls.
- A NULL pointer dereference error in the MulticastSocket implementation.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Feb 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108401
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0412
cve: CVE-2015-0406
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-0403
cve: CVE-2015-0400
cve: CVE-2014-6601
cve: CVE-2014-6587
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72136
url: http://www.securityfocus.com/bid/72154
url: http://www.securityfocus.com/bid/72148
url: http://www.securityfocus.com/bid/72159
url: http://www.securityfocus.com/bid/72132
url: http://www.securityfocus.com/bid/72168
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0308
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Jul 2014) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or possibly other impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

... continued from previous page ...

Affected Software/OS
Oracle Java SE 6 update 75 and prior, 7 update 60 and prior, and 8 update 5.0 and prior on Linux.

Vulnerability Insight
Multiple flaws exist:
- Two unspecified errors related to the Deployment subcomponent.
- An unspecified error in the Hotspot subcomponent related to bytecode verification.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Jul 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108416
Version used: `2024-02-20T14:37:13Z`

References
```
cve: CVE-2014-4265
cve: CVE-2014-4219
cve: CVE-2014-4227
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68603
url: http://www.securityfocus.com/bid/68620
url: http://www.securityfocus.com/bid/68632
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Jul 2014) - Linux

Summary

... continues on next page ...

... continued from previous page ...

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation will allow remote attackers to execute arbitrary code or possibly other impacts.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 75 and prior, 7 update 60 and prior, and 8 update 5.0 and prior on Linux.

Vulnerability Insight

Multiple flaws exist:

- Two unspecified errors related to the Deployment subcomponent.
- An unspecified error in the Hotspot subcomponent related to bytecode verification.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 (Jul 2014) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108416

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-4265
cve: CVE-2014-4219
cve: CVE-2014-4227
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68603
url: http://www.securityfocus.com/bid/68620
url: http://www.securityfocus.com/bid/68632
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 (Feb 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to conduct a denial of service attack, man-in-the-middle attack, potentially disclose memory contents, remove or overwrite arbitrary files on the system, disclose certain directory information, bypass sandbox restrictions and potentially execute arbitrary code.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 75 and prior, 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist due to:
- An infinite loop in the DER decoder that is triggered when handling negative length values.
- An error in the RMI component's transport implementation related to incorrect context class loader use.
- An error in the Swing component's file chooser implementation.
- An error in vm/memory/referenceProcessor.cpp related to handling of phantom object references in the Hotspot JVM garbage collector.
- An error in the Hotspot JVM related to insecure handling of temporary performance data files.
- An error in the JSSE component related to improper ChangeCipherSpec tracking during SSL/TLS handshakes.
- Two out-of-bounds read errors in the layout component that is triggered when parsing fonts.

. . . 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 JRE Multiple Unspecified Vulnerabilities-04 (Feb 2015) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108403

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0410
cve: CVE-2015-0408
cve: CVE-2015-0407
cve: CVE-2015-0395
cve: CVE-2015-0383
cve: CVE-2014-6593
cve: CVE-2014-6591
cve: CVE-2014-6585
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72165
url: http://www.securityfocus.com/bid/72140
url: http://www.securityfocus.com/bid/72162
url: http://www.securityfocus.com/bid/72142
url: http://www.securityfocus.com/bid/72155
url: http://www.securityfocus.com/bid/72169
url: http://www.securityfocus.com/bid/72175
url: http://www.securityfocus.com/bid/72173
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K16/1739
cert-bund: CB-K15/1396
cert-bund: CB-K15/1133
cert-bund: CB-K15/0669
cert-bund: CB-K15/0442
cert-bund: CB-K15/0393
cert-bund: CB-K15/0316
cert-bund: CB-K15/0308
cert-bund: CB-K15/0291
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-1477
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-0701
dfn-cert: DFN-CERT-2015-0465
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0327
dfn-cert: DFN-CERT-2015-0318
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0296
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 (Feb 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to conduct a denial of service attack, man-in-the-middle attack, potentially disclose memory contents, remove or overwrite arbitrary files on the system, disclose certain directory information, bypass sandbox restrictions and potentially execute arbitrary code.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 75 and prior, 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist due to:
- An infinite loop in the DER decoder that is triggered when handling negative length values.
- An error in the RMI component's transport implementation related to incorrect context class loader use.
- An error in the Swing component's file chooser implementation.
- An error in vm/memory/referenceProcessor.cpp related to handling of phantom object references in the Hotspot JVM garbage collector.
- An error in the Hotspot JVM related to insecure handling of temporary performance data files.
- An error in the JSSE component related to improper ChangeCipherSpec tracking during SSL/TLS handshakes.
- Two out-of-bounds read errors in the layout component that is triggered when parsing fonts.

. . . 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 JRE Multiple Unspecified Vulnerabilities-04 (Feb 2015) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108403

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0410
cve: CVE-2015-0408
cve: CVE-2015-0407
cve: CVE-2015-0395
cve: CVE-2015-0383
cve: CVE-2014-6593
cve: CVE-2014-6591
cve: CVE-2014-6585
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72165
url: http://www.securityfocus.com/bid/72140
url: http://www.securityfocus.com/bid/72162
url: http://www.securityfocus.com/bid/72142
url: http://www.securityfocus.com/bid/72155
url: http://www.securityfocus.com/bid/72169
url: http://www.securityfocus.com/bid/72175
url: http://www.securityfocus.com/bid/72173
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K16/1739
cert-bund: CB-K15/1396
cert-bund: CB-K15/1133
cert-bund: CB-K15/0669
cert-bund: CB-K15/0442
cert-bund: CB-K15/0393
cert-bund: CB-K15/0316
cert-bund: CB-K15/0308
cert-bund: CB-K15/0291
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-1477
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-0701
dfn-cert: DFN-CERT-2015-0465
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0327
dfn-cert: DFN-CERT-2015-0318
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0296
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 (Feb 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to conduct a denial of service attack, man-in-the-middle attack, potentially disclose memory contents, remove or overwrite arbitrary files on the system, disclose certain directory information, bypass sandbox restrictions and potentially execute arbitrary code.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 75 and prior, 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist due to:
- An infinite loop in the DER decoder that is triggered when handling negative length values.
- An error in the RMI component's transport implementation related to incorrect context class loader use.
- An error in the Swing component's file chooser implementation.
- An error in vm/memory/referenceProcessor.cpp related to handling of phantom object references in the Hotspot JVM garbage collector.
- An error in the Hotspot JVM related to insecure handling of temporary performance data files.
- An error in the JSSE component related to improper ChangeCipherSpec tracking during SSL/TLS handshakes.
- Two out-of-bounds read errors in the layout component that is triggered when parsing fonts.

. . . 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 JRE Multiple Unspecified Vulnerabilities-04 (Feb 2015) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108403

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0410
cve: CVE-2015-0408
cve: CVE-2015-0407
cve: CVE-2015-0395
cve: CVE-2015-0383
cve: CVE-2014-6593
cve: CVE-2014-6591
cve: CVE-2014-6585
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72165
url: http://www.securityfocus.com/bid/72140
url: http://www.securityfocus.com/bid/72162
url: http://www.securityfocus.com/bid/72142
url: http://www.securityfocus.com/bid/72155
url: http://www.securityfocus.com/bid/72169
url: http://www.securityfocus.com/bid/72175
url: http://www.securityfocus.com/bid/72173
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K16/1739
cert-bund: CB-K15/1396
cert-bund: CB-K15/1133
cert-bund: CB-K15/0669
cert-bund: CB-K15/0442
cert-bund: CB-K15/0393
cert-bund: CB-K15/0316
cert-bund: CB-K15/0308
cert-bund: CB-K15/0291
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-1477
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-0701
dfn-cert: DFN-CERT-2015-0465
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0327
dfn-cert: DFN-CERT-2015-0318
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0296
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-03 (Jan 2014) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

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

Impact
Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior, Java SE 5 update 55 and prior on Linux.

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
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 Multiple Unspecified Vulnerabilities-03 (Jan 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108415
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2013-5884
cve: CVE-2013-5896
cve: CVE-2013-5905
cve: CVE-2013-5906
cve: CVE-2013-5907
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-0368
cve: CVE-2014-0373
cve: CVE-2014-0376
cve: CVE-2014-0411
cve: CVE-2014-0416
cve: CVE-2014-0417
cve: CVE-2014-0422
cve: CVE-2014-0423
cve: CVE-2014-0428
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64894
url: http://www.securityfocus.com/bid/64903
url: http://www.securityfocus.com/bid/64907
url: http://www.securityfocus.com/bid/64914
url: http://www.securityfocus.com/bid/64921
url: http://www.securityfocus.com/bid/64922
url: http://www.securityfocus.com/bid/64924
url: http://www.securityfocus.com/bid/64926
url: http://www.securityfocus.com/bid/64932
url: http://www.securityfocus.com/bid/64934
url: http://www.securityfocus.com/bid/64935
url: http://www.securityfocus.com/bid/64937
url: http://www.securityfocus.com/bid/64918
url: http://www.securityfocus.com/bid/64930
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0572
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0140
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-03 (Jan 2014) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

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 affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior, Java SE 5 update 55 and prior on Linux.

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
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 Multiple Unspecified Vulnerabilities-03 (Jan 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108415
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2013-5884
cve: CVE-2013-5896
cve: CVE-2013-5905
cve: CVE-2013-5906
cve: CVE-2013-5907
cve: CVE-2014-0368
cve: CVE-2014-0373
cve: CVE-2014-0376
cve: CVE-2014-0411
cve: CVE-2014-0416
cve: CVE-2014-0417
cve: CVE-2014-0422
cve: CVE-2014-0423
cve: CVE-2014-0428
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64894
url: http://www.securityfocus.com/bid/64903
url: http://www.securityfocus.com/bid/64907
url: http://www.securityfocus.com/bid/64914
url: http://www.securityfocus.com/bid/64921
url: http://www.securityfocus.com/bid/64922
url: http://www.securityfocus.com/bid/64924
url: http://www.securityfocus.com/bid/64926
url: http://www.securityfocus.com/bid/64932
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/64934
url: http://www.securityfocus.com/bid/64935
url: http://www.securityfocus.com/bid/64937
url: http://www.securityfocus.com/bid/64918
url: http://www.securityfocus.com/bid/64930
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0572
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0140
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-03 (Jan 2014) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior, Java SE 5 update 55 and prior on Linux.

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
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 Multiple Unspecified Vulnerabilities-03 (Jan 2014) - Linux`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.108415
Version used: 2024-02-20T14:37:13Z

References

```
cve: CVE-2013-5884
cve: CVE-2013-5896
cve: CVE-2013-5905
cve: CVE-2013-5906
cve: CVE-2013-5907
cve: CVE-2014-0368
cve: CVE-2014-0373
cve: CVE-2014-0376
cve: CVE-2014-0411
cve: CVE-2014-0416
cve: CVE-2014-0417
cve: CVE-2014-0422
cve: CVE-2014-0423
cve: CVE-2014-0428
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64894
url: http://www.securityfocus.com/bid/64903
url: http://www.securityfocus.com/bid/64907
url: http://www.securityfocus.com/bid/64914
url: http://www.securityfocus.com/bid/64921
url: http://www.securityfocus.com/bid/64922
url: http://www.securityfocus.com/bid/64924
url: http://www.securityfocus.com/bid/64926
url: http://www.securityfocus.com/bid/64932
url: http://www.securityfocus.com/bid/64934
url: http://www.securityfocus.com/bid/64935
url: http://www.securityfocus.com/bid/64937
url: http://www.securityfocus.com/bid/64918
url: http://www.securityfocus.com/bid/64930
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0572
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0140
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-02 (Jan 2014) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

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

Impact
Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior on Linux

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
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 Multiple Unspecified Vulnerabilities-02 (Jan 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108412
Version used: `2024-02-20T14:37:13Z`

References
```
cve: CVE-2013-5878
cve: CVE-2013-5887
cve: CVE-2013-5888
cve: CVE-2013-5889
cve: CVE-2013-5898
cve: CVE-2013-5899
cve: CVE-2013-5902
cve: CVE-2013-5910
cve: CVE-2014-0375
cve: CVE-2014-0410
cve: CVE-2014-0403
cve: CVE-2014-0415
cve: CVE-2014-0418
cve: CVE-2014-0424
cve: CVE-2014-0387
url: http://secunia.com/advisories/56485
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/64875
url: http://www.securityfocus.com/bid/64882
url: http://www.securityfocus.com/bid/64899
url: http://www.securityfocus.com/bid/64912
url: http://www.securityfocus.com/bid/64915
url: http://www.securityfocus.com/bid/64916
url: http://www.securityfocus.com/bid/64917
url: http://www.securityfocus.com/bid/64919
url: http://www.securityfocus.com/bid/64920
url: http://www.securityfocus.com/bid/64923
url: http://www.securityfocus.com/bid/64925
url: http://www.securityfocus.com/bid/64928
url: http://www.securityfocus.com/bid/64931
url: http://www.securityfocus.com/bid/64933
url: http://www.securityfocus.com/bid/64927
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-02 (Jan 2014) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior on Linux

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple unspecified vulnerabilities exist.

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 Multiple Unspecified Vulnerabilities-02 (Jan 2014) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108412

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2013-5878
cve: CVE-2013-5887
cve: CVE-2013-5888
cve: CVE-2013-5889
cve: CVE-2013-5898
cve: CVE-2013-5899
cve: CVE-2013-5902
cve: CVE-2013-5910
cve: CVE-2014-0375
cve: CVE-2014-0410
cve: CVE-2014-0403
cve: CVE-2014-0415
cve: CVE-2014-0418
cve: CVE-2014-0424
cve: CVE-2014-0387
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64875
url: http://www.securityfocus.com/bid/64882
url: http://www.securityfocus.com/bid/64899
url: http://www.securityfocus.com/bid/64912
url: http://www.securityfocus.com/bid/64915
url: http://www.securityfocus.com/bid/64916
url: http://www.securityfocus.com/bid/64917
url: http://www.securityfocus.com/bid/64919
url: http://www.securityfocus.com/bid/64920
url: http://www.securityfocus.com/bid/64923
url: http://www.securityfocus.com/bid/64925
url: http://www.securityfocus.com/bid/64928
url: http://www.securityfocus.com/bid/64931
url: http://www.securityfocus.com/bid/64933
url: http://www.securityfocus.com/bid/64927
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/0141
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-02 (Jan 2014) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior on Linux

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
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 Multiple Unspecified Vulnerabilities-02 (Jan 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108412
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2013-5878
cve: CVE-2013-5887
cve: CVE-2013-5888
cve: CVE-2013-5889
cve: CVE-2013-5898
cve: CVE-2013-5899
cve: CVE-2013-5902
cve: CVE-2013-5910
cve: CVE-2014-0375
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-0410
cve: CVE-2014-0403
cve: CVE-2014-0415
cve: CVE-2014-0418
cve: CVE-2014-0424
cve: CVE-2014-0387
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64875
url: http://www.securityfocus.com/bid/64882
url: http://www.securityfocus.com/bid/64899
url: http://www.securityfocus.com/bid/64912
url: http://www.securityfocus.com/bid/64915
url: http://www.securityfocus.com/bid/64916
url: http://www.securityfocus.com/bid/64917
url: http://www.securityfocus.com/bid/64919
url: http://www.securityfocus.com/bid/64920
url: http://www.securityfocus.com/bid/64923
url: http://www.securityfocus.com/bid/64925
url: http://www.securityfocus.com/bid/64928
url: http://www.securityfocus.com/bid/64931
url: http://www.securityfocus.com/bid/64933
url: http://www.securityfocus.com/bid/64927
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
```

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

Summary
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Vulnerability Detection Result

```
The "Ubuntu" Operating System on the remote host has reached the end of life.
CPE:               cpe:/o:canonical:ubuntu_linux:14.04:-:lts
Installed version,
build or SP:       14.04
EOL date:          2024-04-01
EOL info:          https://wiki.ubuntu.com/Releases
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

An EOL version of an OS 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: Mitigation

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method

Checks if an EOL version of an OS is present on the target host.

Details: `Operating System (OS) End of Life (EOL) Detection`

OID:1.3.6.1.4.1.25623.1.0.103674

Version used: `2024-02-28T14:37:42Z`

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:

Solution type: VendorFix

Update to the latest available stable release for your scan environment.

. . . continues on next page . . .

. . . continued from previous page . . .

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: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch from the referenced advisory.
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow 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 Java SE 6 update 95, 7 update 80, 8 update 45 on Linux.

Vulnerability Insight
Multiple errors exist due to unspecified flaws related to multiple unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108395
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-4760
cve: CVE-2015-4749
cve: CVE-2015-4748
cve: CVE-2015-4733
cve: CVE-2015-4732
cve: CVE-2015-4731
cve: CVE-2015-2664
cve: CVE-2015-2638
cve: CVE-2015-2637
cve: CVE-2015-2621
cve: CVE-2015-2625
cve: CVE-2015-2627
cve: CVE-2015-2628
cve: CVE-2015-2632
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-2601
cve: CVE-2015-2590
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75784
url: http://www.securityfocus.com/bid/75890
url: http://www.securityfocus.com/bid/75854
url: http://www.securityfocus.com/bid/75832
url: http://www.securityfocus.com/bid/75823
url: http://www.securityfocus.com/bid/75812
url: http://www.securityfocus.com/bid/75857
url: http://www.securityfocus.com/bid/75833
url: http://www.securityfocus.com/bid/75883
url: http://www.securityfocus.com/bid/75874
url: http://www.securityfocus.com/bid/75895
url: http://www.securityfocus.com/bid/75893
url: http://www.securityfocus.com/bid/75796
url: http://www.securityfocus.com/bid/75861
url: http://www.securityfocus.com/bid/75867
url: http://www.securityfocus.com/bid/75818
cert-bund: CB-K16/1842
cert-bund: CB-K16/0617
cert-bund: CB-K15/1751
cert-bund: CB-K15/1352
cert-bund: CB-K15/1302
cert-bund: CB-K15/1250
cert-bund: CB-K15/1249
cert-bund: CB-K15/1197
cert-bund: CB-K15/1148
cert-bund: CB-K15/1136
cert-bund: CB-K15/1133
cert-bund: CB-K15/1090
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1427
dfn-cert: DFN-CERT-2015-1373
dfn-cert: DFN-CERT-2015-1320
dfn-cert: DFN-CERT-2015-1318
dfn-cert: DFN-CERT-2015-1269
dfn-cert: DFN-CERT-2015-1206
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch from the referenced advisory.
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow 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 Java SE 6 update 95, 7 update 80, 8 update 45 on Linux.

Vulnerability Insight
Multiple errors exist due to unspecified flaws related to multiple unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108395
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-4760
cve: CVE-2015-4749
cve: CVE-2015-4748
cve: CVE-2015-4733
cve: CVE-2015-4732
cve: CVE-2015-4731
cve: CVE-2015-2664
cve: CVE-2015-2638
cve: CVE-2015-2637
cve: CVE-2015-2621
cve: CVE-2015-2625
cve: CVE-2015-2627
cve: CVE-2015-2628
cve: CVE-2015-2632
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-2601
cve: CVE-2015-2590
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75784
url: http://www.securityfocus.com/bid/75890
url: http://www.securityfocus.com/bid/75854
url: http://www.securityfocus.com/bid/75832
url: http://www.securityfocus.com/bid/75823
url: http://www.securityfocus.com/bid/75812
url: http://www.securityfocus.com/bid/75857
url: http://www.securityfocus.com/bid/75833
url: http://www.securityfocus.com/bid/75883
url: http://www.securityfocus.com/bid/75874
url: http://www.securityfocus.com/bid/75895
url: http://www.securityfocus.com/bid/75893
url: http://www.securityfocus.com/bid/75796
url: http://www.securityfocus.com/bid/75861
url: http://www.securityfocus.com/bid/75867
url: http://www.securityfocus.com/bid/75818
cert-bund: CB-K16/1842
cert-bund: CB-K16/0617
cert-bund: CB-K15/1751
cert-bund: CB-K15/1352
cert-bund: CB-K15/1302
cert-bund: CB-K15/1250
cert-bund: CB-K15/1249
cert-bund: CB-K15/1197
cert-bund: CB-K15/1148
cert-bund: CB-K15/1136
cert-bund: CB-K15/1133
cert-bund: CB-K15/1090
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1427
dfn-cert: DFN-CERT-2015-1373
dfn-cert: DFN-CERT-2015-1320
dfn-cert: DFN-CERT-2015-1318
dfn-cert: DFN-CERT-2015-1269
dfn-cert: DFN-CERT-2015-1206
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch from the referenced advisory.
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation will allow 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 Java SE 6 update 95, 7 update 80, 8 update 45 on Linux.

Vulnerability Insight
Multiple errors exist due to unspecified flaws related to multiple unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108395
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-4760
cve: CVE-2015-4749
cve: CVE-2015-4748
cve: CVE-2015-4733
cve: CVE-2015-4732
cve: CVE-2015-4731
cve: CVE-2015-2664
cve: CVE-2015-2638
cve: CVE-2015-2637
cve: CVE-2015-2621
cve: CVE-2015-2625
cve: CVE-2015-2627
cve: CVE-2015-2628
cve: CVE-2015-2632
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-2601
cve: CVE-2015-2590
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75784
url: http://www.securityfocus.com/bid/75890
url: http://www.securityfocus.com/bid/75854
url: http://www.securityfocus.com/bid/75832
url: http://www.securityfocus.com/bid/75823
url: http://www.securityfocus.com/bid/75812
url: http://www.securityfocus.com/bid/75857
url: http://www.securityfocus.com/bid/75833
url: http://www.securityfocus.com/bid/75883
url: http://www.securityfocus.com/bid/75874
url: http://www.securityfocus.com/bid/75895
url: http://www.securityfocus.com/bid/75893
url: http://www.securityfocus.com/bid/75796
url: http://www.securityfocus.com/bid/75861
url: http://www.securityfocus.com/bid/75867
url: http://www.securityfocus.com/bid/75818
cert-bund: CB-K16/1842
cert-bund: CB-K16/0617
cert-bund: CB-K15/1751
cert-bund: CB-K15/1352
cert-bund: CB-K15/1302
cert-bund: CB-K15/1250
cert-bund: CB-K15/1249
cert-bund: CB-K15/1197
cert-bund: CB-K15/1148
cert-bund: CB-K15/1136
cert-bund: CB-K15/1133
cert-bund: CB-K15/1090
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1427
dfn-cert: DFN-CERT-2015-1373
dfn-cert: DFN-CERT-2015-1320
dfn-cert: DFN-CERT-2015-1318
dfn-cert: DFN-CERT-2015-1269
dfn-cert: DFN-CERT-2015-1206
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Apr 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to gain knowledge of potentially sensitive information, conduct denial-of-service attacks, execute arbitrary code and other unspecified impact.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5.0 update 81 and prior, 6 update 91 and prior, 7 update 76 and prior, and 8 update 40 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- An error in the Java Cryptography Extension (JCE) subcomponent's RSA signature implementation.
- An error in the JSSE subcomponent that is triggered when checking X.509 certificate options.
- An error in the 'ReferenceProcessor::process_discovered_references' function in share/vm/memory/referenceProcessor.cpp script.
- Two unspecified errors related to the 2D subcomponent.
- An error in the Beans subcomponent related to permissions and resource loading.
- An off-by-one overflow condition in the functions 'LigatureSubstitutionProcessor::processStateEntry' and 'LigatureSubstitutionProcessor2::processStateEntry' within LigatureSubstProc.cpp and LigatureSubstProc2.cpp scripts respectively.
- An unspecified error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Apr 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108397
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0491
cve: CVE-2015-0488
cve: CVE-2015-0480
cve: CVE-2015-0478
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-0477
cve: CVE-2015-0469
cve: CVE-2015-0460
cve: CVE-2015-0459
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74094
url: http://www.securityfocus.com/bid/74111
url: http://www.securityfocus.com/bid/74104
url: http://www.securityfocus.com/bid/74147
url: http://www.securityfocus.com/bid/74119
url: http://www.securityfocus.com/bid/74072
url: http://www.securityfocus.com/bid/74097
url: http://www.securityfocus.com/bid/74083
cert-bund: CB-K15/1751
cert-bund: CB-K15/1090
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0529
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0554
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Apr 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to gain knowledge of potentially sensitive information, conduct denial-of-service attacks, execute arbitrary code and other unspecified impact.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5.0 update 81 and prior, 6 update 91 and prior, 7 update 76 and prior, and 8 update 40 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- An error in the Java Cryptography Extension (JCE) subcomponent's RSA signature implementation.
- An error in the JSSE subcomponent that is triggered when checking X.509 certificate options.
- An error in the 'ReferenceProcessor::process_discovered_references' function in share/vm/memory/referenceProcessor.cpp script.
- Two unspecified errors related to the 2D subcomponent.
- An error in the Beans subcomponent related to permissions and resource loading.
- An off-by-one overflow condition in the functions 'LigatureSubstitutionProcessor::processStateEntry' and 'LigatureSubstitutionProcessor2::processStateEntry' within LigatureSubstProc.cpp and LigatureSubstProc2.cpp scripts respectively.
- An unspecified error.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Apr 2015) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108397

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0491
cve: CVE-2015-0488
cve: CVE-2015-0480
cve: CVE-2015-0478
cve: CVE-2015-0477
cve: CVE-2015-0469
cve: CVE-2015-0460
cve: CVE-2015-0459
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74094
url: http://www.securityfocus.com/bid/74111
url: http://www.securityfocus.com/bid/74104
url: http://www.securityfocus.com/bid/74147
url: http://www.securityfocus.com/bid/74119
url: http://www.securityfocus.com/bid/74072
url: http://www.securityfocus.com/bid/74097
url: http://www.securityfocus.com/bid/74083
cert-bund: CB-K15/1751
cert-bund: CB-K15/1090
```

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0529
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0554
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Apr 2015) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to gain knowledge of potentially sensitive information, conduct denial-of-service attacks, execute arbitrary code and other unspecified impact.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5.0 update 81 and prior, 6 update 91 and prior, 7 update 76 and prior, and 8 update 40 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- An error in the Java Cryptography Extension (JCE) subcomponent's RSA signature implementation.
- An error in the JSSE subcomponent that is triggered when checking X.509 certificate options.
- An error in the 'ReferenceProcessor::process_discovered_references' function in share/vm/memory/referenceProcessor.cpp script.
- Two unspecified errors related to the 2D subcomponent.

... continues on next page ...

. . . continued from previous page . . .

- An error in the Beans subcomponent related to permissions and resource loading.
- An off-by-one overflow condition in the functions 'LigatureSubstitutionProcessor::processStateEntry' and 'LigatureSubstitutionProcessor2::processStateEntry' within LigatureSubstProc.cpp and LigatureSubstProc2.cpp scripts respectively.
- An unspecified error.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Apr 2015) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108397

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0491
cve: CVE-2015-0488
cve: CVE-2015-0480
cve: CVE-2015-0478
cve: CVE-2015-0477
cve: CVE-2015-0469
cve: CVE-2015-0460
cve: CVE-2015-0459
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74094
url: http://www.securityfocus.com/bid/74111
url: http://www.securityfocus.com/bid/74104
url: http://www.securityfocus.com/bid/74147
url: http://www.securityfocus.com/bid/74119
url: http://www.securityfocus.com/bid/74072
url: http://www.securityfocus.com/bid/74097
url: http://www.securityfocus.com/bid/74083
cert-bund: CB-K15/1751
cert-bund: CB-K15/1090
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0529
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0554
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2014) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow attackers to perform certain actions with escalated privileges, disclose sensitive information and compromise a user's system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors related to the Deployment subcomponent.
- An XXE (Xml eXternal Entity) injection error in com/sun/org/apache/xerces/internal/impl/XMLEntityManager.j
script.
- An error in windows/native/sun/awt/splashscreen/splashscreen_sys.c script related to handling of splash images.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 (Oct 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108414
Version used: `2024-02-20T14:37:13Z`

References
```
cve: CVE-2014-6532
cve: CVE-2014-6517
cve: CVE-2014-6515
cve: CVE-2014-6513
cve: CVE-2014-6503
cve: CVE-2014-6493
cve: CVE-2014-6492
cve: CVE-2014-6466
cve: CVE-2014-6458
cve: CVE-2014-4288
url: http://secunia.com/advisories/61609/
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/70456
url: http://www.securityfocus.com/bid/70460
url: http://www.securityfocus.com/bid/70468
url: http://www.securityfocus.com/bid/70470
url: http://www.securityfocus.com/bid/70484
url: http://www.securityfocus.com/bid/70507
url: http://www.securityfocus.com/bid/70518
url: http://www.securityfocus.com/bid/70552
url: http://www.securityfocus.com/bid/70565
url: http://www.securityfocus.com/bid/70569
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 9.8)
NVT: Oracle Java SE Security Update (cpuoct2017 - 03) - Linux

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation of this vulnerability will allow attackers to partially modify data by leveraging improper pointer arithmetic within the application.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier.

Vulnerability Insight
Multiple flaws exist due to a flaw in Util (zlib) component of the application.

. . . 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 (cpuoct2017 - 03) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108380

Version used: `2022-06-24T09:38:38Z`

References

```
cve: CVE-2016-9841
url: https://www.oracle.com/security-alerts/cpuoct2017.html
url: http://www.securityfocus.com/bid/95131
cert-bund: WID-SEC-2024-1232
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1005
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
dfn-cert: DFN-CERT-2024-0998
dfn-cert: DFN-CERT-2019-0592
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2018-2435
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 Java SE Security Update (cpuoct2017 - 03) - Linux

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation of this vulnerability will allow attackers to partially modify data by leveraging improper pointer arithmetic within the application.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier.

Vulnerability Insight
Multiple flaws exist due to a flaw in Util (zlib) component of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (cpuoct2017 - 03) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108380
Version used: `2022-06-24T09:38:38Z`

References

```
cve: CVE-2016-9841
url: https://www.oracle.com/security-alerts/cpuoct2017.html
url: http://www.securityfocus.com/bid/95131
cert-bund: WID-SEC-2024-1232
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1005
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0784
cert-bund: CB-K16/1996
dfn-cert: DFN-CERT-2024-0998
dfn-cert: DFN-CERT-2019-0592
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2018-2435
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 Java SE Security Update (cpuoct2017 - 03) - Linux

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation of this vulnerability will allow attackers to partially modify data by leveraging improper pointer arithmetic within the application.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier.

Vulnerability Insight
Multiple flaws exist due to a flaw in Util (zlib) component of the application.

. . . 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 (cpuoct2017 - 03) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108380
Version used: `2022-06-24T09:38:38Z`

References

```
cve: CVE-2016-9841
url: https://www.oracle.com/security-alerts/cpuoct2017.html
url: http://www.securityfocus.com/bid/95131
cert-bund: WID-SEC-2024-1232
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1005
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
dfn-cert: DFN-CERT-2024-0998
dfn-cert: DFN-CERT-2019-0592
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2018-2435
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: 9.6)
NVT: Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to gain elevated privileges, partially access and partially modify data, access sensitive data, obtain sensitive information or cause a denial of service, .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier, 9.0 on Linux.

Vulnerability Insight
Multiple flaws exist due to flaws in the 'Hotspot', 'RMI ', 'Libraries', 'Smart Card IO', 'Security', 'Javadoc', 'JAXP', 'Serialization' and 'Networking' components of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108379
Version used: `2022-08-01T10:11:45Z`

References

```
cve: CVE-2017-10388
cve: CVE-2017-10293
cve: CVE-2017-10346
cve: CVE-2017-10345
cve: CVE-2017-10285
cve: CVE-2017-10356
cve: CVE-2017-10348
cve: CVE-2017-10295
cve: CVE-2017-10349
cve: CVE-2017-10347
cve: CVE-2017-10274
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-10355
cve: CVE-2017-10357
cve: CVE-2017-10281
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101321
url: http://www.securityfocus.com/bid/101338
url: http://www.securityfocus.com/bid/101315
url: http://www.securityfocus.com/bid/101396
url: http://www.securityfocus.com/bid/101319
url: http://www.securityfocus.com/bid/101413
url: http://www.securityfocus.com/bid/101354
url: http://www.securityfocus.com/bid/101384
url: http://www.securityfocus.com/bid/101348
url: http://www.securityfocus.com/bid/101382
url: http://www.securityfocus.com/bid/101333
url: http://www.securityfocus.com/bid/101369
url: http://www.securityfocus.com/bid/101355
url: http://www.securityfocus.com/bid/101378
cert-bund: CB-K18/0715
cert-bund: CB-K18/0570
cert-bund: CB-K18/0495
cert-bund: CB-K18/0301
cert-bund: CB-K18/0030
cert-bund: CB-K17/2199
cert-bund: CB-K17/2168
cert-bund: CB-K17/2106
cert-bund: CB-K17/2047
cert-bund: CB-K17/1745
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0691
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0643
dfn-cert: DFN-CERT-2018-0536
dfn-cert: DFN-CERT-2018-0318
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-2203
dfn-cert: DFN-CERT-2017-2135
dfn-cert: DFN-CERT-2017-1825
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to gain elevated privileges, partially access and partially modify data, access sensitive data, obtain sensitive information or cause a denial of service, .

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier, 9.0 on Linux.

Vulnerability Insight

Multiple flaws exist due to flaws in the 'Hotspot', 'RMI ', 'Libraries', 'Smart Card IO', 'Security', 'Javadoc', 'JAXP', 'Serialization' and 'Networking' components of the application.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108379

Version used: `2022-08-01T10:11:45Z`

References

```
cve: CVE-2017-10388
cve: CVE-2017-10293
cve: CVE-2017-10346
cve: CVE-2017-10345
cve: CVE-2017-10285
cve: CVE-2017-10356
cve: CVE-2017-10348
cve: CVE-2017-10295
cve: CVE-2017-10349
cve: CVE-2017-10347
cve: CVE-2017-10274
cve: CVE-2017-10355
cve: CVE-2017-10357
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-10281
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101321
url: http://www.securityfocus.com/bid/101338
url: http://www.securityfocus.com/bid/101315
url: http://www.securityfocus.com/bid/101396
url: http://www.securityfocus.com/bid/101319
url: http://www.securityfocus.com/bid/101413
url: http://www.securityfocus.com/bid/101354
url: http://www.securityfocus.com/bid/101384
url: http://www.securityfocus.com/bid/101348
url: http://www.securityfocus.com/bid/101382
url: http://www.securityfocus.com/bid/101333
url: http://www.securityfocus.com/bid/101369
url: http://www.securityfocus.com/bid/101355
url: http://www.securityfocus.com/bid/101378
cert-bund: CB-K18/0715
cert-bund: CB-K18/0570
cert-bund: CB-K18/0495
cert-bund: CB-K18/0301
cert-bund: CB-K18/0030
cert-bund: CB-K17/2199
cert-bund: CB-K17/2168
cert-bund: CB-K17/2106
cert-bund: CB-K17/2047
cert-bund: CB-K17/1745
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0691
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0643
dfn-cert: DFN-CERT-2018-0536
dfn-cert: DFN-CERT-2018-0318
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-2203
dfn-cert: DFN-CERT-2017-2135
dfn-cert: DFN-CERT-2017-1825
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux

Summary

Oracle Java SE is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

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 Java SE version 1.6.0.151 and earlier, 1.7.0.141 and earlier, 1.8.0.131 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to multiple unspecifide errors in 'Security', 'AWT', 'ImageIO', 'JAXP', 'Libraries', 'RMI', 'Hotspot', 'JCE', 'JAX-WS', '2D', 'Serialization', 'Deployment' component of the application.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108375

Version used: `2023-03-24T10:19:42Z`

References

```
cve: CVE-2017-10198
cve: CVE-2017-10096
cve: CVE-2017-10135
cve: CVE-2017-10110
cve: CVE-2017-10115
cve: CVE-2017-10116
cve: CVE-2017-10074
cve: CVE-2017-10053
cve: CVE-2017-10087
cve: CVE-2017-10089
cve: CVE-2017-10243
cve: CVE-2017-10102
cve: CVE-2017-10101
cve: CVE-2017-10107
cve: CVE-2017-10109
cve: CVE-2017-10105
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-10081
cve: CVE-2017-10193
cve: CVE-2017-10067
cve: CVE-2017-10108
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
url: http://www.securityfocus.com/bid/99818
url: http://www.securityfocus.com/bid/99670
url: http://www.securityfocus.com/bid/99839
url: http://www.securityfocus.com/bid/99643
url: http://www.securityfocus.com/bid/99774
url: http://www.securityfocus.com/bid/99734
url: http://www.securityfocus.com/bid/99731
url: http://www.securityfocus.com/bid/99842
url: http://www.securityfocus.com/bid/99703
url: http://www.securityfocus.com/bid/99659
url: http://www.securityfocus.com/bid/99827
url: http://www.securityfocus.com/bid/99712
url: http://www.securityfocus.com/bid/99674
url: http://www.securityfocus.com/bid/99719
url: http://www.securityfocus.com/bid/99847
url: http://www.securityfocus.com/bid/99851
url: http://www.securityfocus.com/bid/99853
url: http://www.securityfocus.com/bid/99854
url: http://www.securityfocus.com/bid/99756
url: http://www.securityfocus.com/bid/99846
cert-bund: CB-K18/0030
cert-bund: CB-K18/0015
cert-bund: CB-K17/2168
cert-bund: CB-K17/1699
cert-bund: CB-K17/1496
cert-bund: CB-K17/1477
cert-bund: CB-K17/1470
cert-bund: CB-K17/1375
cert-bund: CB-K17/1199
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2018-0014
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1775
dfn-cert: DFN-CERT-2017-1561
dfn-cert: DFN-CERT-2017-1543
dfn-cert: DFN-CERT-2017-1536
dfn-cert: DFN-CERT-2017-1438
dfn-cert: DFN-CERT-2017-1241
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

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 Java SE version 1.6.0.151 and earlier, 1.7.0.141 and earlier, 1.8.0.131 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecifide errors in 'Security', 'AWT', 'ImageIO', 'JAXP', 'Libraries', 'RMI', 'Hotspot', 'JCE', 'JAX-WS', '2D', 'Serialization', 'Deployment' component of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108375
Version used: `2023-03-24T10:19:42Z`

References

```
cve: CVE-2017-10198
cve: CVE-2017-10096
cve: CVE-2017-10135
cve: CVE-2017-10110
cve: CVE-2017-10115
cve: CVE-2017-10116
cve: CVE-2017-10074
cve: CVE-2017-10053
cve: CVE-2017-10087
cve: CVE-2017-10089
cve: CVE-2017-10243
cve: CVE-2017-10102
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-10101
cve: CVE-2017-10107
cve: CVE-2017-10109
cve: CVE-2017-10105
cve: CVE-2017-10081
cve: CVE-2017-10193
cve: CVE-2017-10067
cve: CVE-2017-10108
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
url: http://www.securityfocus.com/bid/99818
url: http://www.securityfocus.com/bid/99670
url: http://www.securityfocus.com/bid/99839
url: http://www.securityfocus.com/bid/99643
url: http://www.securityfocus.com/bid/99774
url: http://www.securityfocus.com/bid/99734
url: http://www.securityfocus.com/bid/99731
url: http://www.securityfocus.com/bid/99842
url: http://www.securityfocus.com/bid/99703
url: http://www.securityfocus.com/bid/99659
url: http://www.securityfocus.com/bid/99827
url: http://www.securityfocus.com/bid/99712
url: http://www.securityfocus.com/bid/99674
url: http://www.securityfocus.com/bid/99719
url: http://www.securityfocus.com/bid/99847
url: http://www.securityfocus.com/bid/99851
url: http://www.securityfocus.com/bid/99853
url: http://www.securityfocus.com/bid/99854
url: http://www.securityfocus.com/bid/99756
url: http://www.securityfocus.com/bid/99846
cert-bund: CB-K18/0030
cert-bund: CB-K18/0015
cert-bund: CB-K17/2168
cert-bund: CB-K17/1699
cert-bund: CB-K17/1496
cert-bund: CB-K17/1477
cert-bund: CB-K17/1470
cert-bund: CB-K17/1375
cert-bund: CB-K17/1199
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2018-0014
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1775
dfn-cert: DFN-CERT-2017-1561
dfn-cert: DFN-CERT-2017-1543
dfn-cert: DFN-CERT-2017-1536
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1438
dfn-cert: DFN-CERT-2017-1241
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Oct 2016) - Linux

Summary
Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow remote user to access and modify data on the target system, also can obtain elevated privileges on the target system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 121 and prior, 7 update 111 and prior, and 8 update 102 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to:
- A flaw in the 2D component.
- A flaw in the AWT component.
- A flaw in the Hotspot component.
- A flaw in the Networking component.
- A flaw in the JMX component.
- A flaw in the Libraries component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Oct 2016) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108385
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-5556
cve: CVE-2016-5568
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-5582
cve: CVE-2016-5573
cve: CVE-2016-5597
cve: CVE-2016-5554
cve: CVE-2016-5542
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
url: http://www.securityfocus.com/bid/93618
url: http://www.securityfocus.com/bid/93621
url: http://www.securityfocus.com/bid/93623
url: http://www.securityfocus.com/bid/93628
cert-bund: CB-K17/0895
cert-bund: CB-K17/0892
cert-bund: CB-K17/0874
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0456
cert-bund: CB-K17/0055
cert-bund: CB-K16/1802
cert-bund: CB-K16/1615
dfn-cert: DFN-CERT-2017-0921
dfn-cert: DFN-CERT-2017-0920
dfn-cert: DFN-CERT-2017-0903
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0471
dfn-cert: DFN-CERT-2017-0060
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation of this vulnerability will allow attackers to cause some unspecified impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

... continued from previous page ...

Affected Software/OS

Oracle Java SE version 1.6.0.131 and earlier, 1.7.0.121 and earlier, 1.8.0.112 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to multiple unspecified errors in 'Libraries', 'RMI', '2D', 'JAAS', 'Networking' and 'Deployment' sub-components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108372
Version used: `2022-05-19T11:50:09Z`

References

```
cve: CVE-2016-2183
cve: CVE-2017-3231
cve: CVE-2017-3261
cve: CVE-2016-5548
cve: CVE-2017-3253
cve: CVE-2017-3272
cve: CVE-2017-3252
cve: CVE-2017-3259
cve: CVE-2016-5552
cve: CVE-2016-5546
cve: CVE-2017-3241
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/92630
url: http://www.securityfocus.com/bid/95563
url: http://www.securityfocus.com/bid/95566
url: http://www.securityfocus.com/bid/95559
url: http://www.securityfocus.com/bid/95498
url: http://www.securityfocus.com/bid/95533
url: http://www.securityfocus.com/bid/95509
url: http://www.securityfocus.com/bid/95570
url: http://www.securityfocus.com/bid/95512
url: http://www.securityfocus.com/bid/95506
url: http://www.securityfocus.com/bid/95488
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
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
```

... continues on next page ...

... continued from previous page ...

```
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-K17/1753
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-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0892
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
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0211
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
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
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
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-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0920
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
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0216
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation of this vulnerability will allow attackers to cause some unspecified impacts.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.131 and earlier, 1.7.0.121 and earlier, 1.8.0.112 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in 'Libraries', 'RMI', '2D', 'JAAS', 'Networking' and 'Deployment' sub-components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108372
Version used: `2022-05-19T11:50:09Z`

References

```
cve: CVE-2016-2183
cve: CVE-2017-3231
cve: CVE-2017-3261
cve: CVE-2016-5548
cve: CVE-2017-3253
cve: CVE-2017-3272
cve: CVE-2017-3252
cve: CVE-2017-3259
cve: CVE-2016-5552
cve: CVE-2016-5546
cve: CVE-2017-3241
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/92630
url: http://www.securityfocus.com/bid/95563
url: http://www.securityfocus.com/bid/95566
url: http://www.securityfocus.com/bid/95559
url: http://www.securityfocus.com/bid/95498
url: http://www.securityfocus.com/bid/95533
url: http://www.securityfocus.com/bid/95509
url: http://www.securityfocus.com/bid/95570
url: http://www.securityfocus.com/bid/95512
url: http://www.securityfocus.com/bid/95506
url: http://www.securityfocus.com/bid/95488
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
```

. . . continues on next page . . .

. . . continued from previous page . . .

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-K17/1753
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-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0892
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
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0211
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
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-2017-1831
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-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0920
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
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0216
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation of this vulnerability will allow attackers to cause some unspecified impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.131 and earlier, 1.7.0.121 and earlier, 1.8.0.112 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in 'Libraries', 'RMI', '2D', 'JAAS', 'Networking' and 'Deployment' sub-components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108372
Version used: `2022-05-19T11:50:09Z`

References

```
cve: CVE-2016-2183
cve: CVE-2017-3231
cve: CVE-2017-3261
cve: CVE-2016-5548
cve: CVE-2017-3253
cve: CVE-2017-3272
cve: CVE-2017-3252
cve: CVE-2017-3259
cve: CVE-2016-5552
cve: CVE-2016-5546
cve: CVE-2017-3241
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/92630
url: http://www.securityfocus.com/bid/95563
url: http://www.securityfocus.com/bid/95566
url: http://www.securityfocus.com/bid/95559
url: http://www.securityfocus.com/bid/95498
url: http://www.securityfocus.com/bid/95533
url: http://www.securityfocus.com/bid/95509
url: http://www.securityfocus.com/bid/95570
url: http://www.securityfocus.com/bid/95512
url: http://www.securityfocus.com/bid/95506
url: http://www.securityfocus.com/bid/95488
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-K17/1753
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-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0892
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
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0211
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-2017-1831
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-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0920
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
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0216
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Vulnerabilities (Apr 2016) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

path / port: /usr/bin/java

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via different vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 113 and prior, 7 update 99 and prior and 8 update 77 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- The Security component in 'OpenJDK' failed to check the digest algorithm strength when generating DSA signatures.
- The JAXP component in 'OpenJDK' failed to properly handle Unicode surrogate pairs used as part of the XML attribute values.
- The RMI server implementation in the JMX component in 'OpenJDK' did not restrict which classes can be deserialized when deserializing authentication credentials.
- Multiple unspecified vulnerabilities.

Vulnerability Detection Method

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

Details: `Oracle Java SE Multiple Vulnerabilities (Apr 2016) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108388

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-0695
cve: CVE-2016-0687
cve: CVE-2016-0686
cve: CVE-2016-3443
cve: CVE-2016-3427
cve: CVE-2016-3425
cve: CVE-2016-3422
cve: CVE-2016-3449
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.ht
↪ml
cert-bund: WID-SEC-2023-1214
cert-bund: CB-K17/0796
cert-bund: CB-K17/0090
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/1080
cert-bund: CB-K16/0800
cert-bund: CB-K16/0726
cert-bund: CB-K16/0634
cert-bund: CB-K16/0594
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-0640
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Vulnerabilities (Apr 2016) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via different vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 113 and prior, 7 update 99 and prior and 8 update 77 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- The Security component in 'OpenJDK' failed to check the digest algorithm strength when generating DSA signatures.
- The JAXP component in 'OpenJDK' failed to properly handle Unicode surrogate pairs used as part of the XML attribute values.
- The RMI server implementation in the JMX component in 'OpenJDK' did not restrict which classes can be deserialized when deserializing authentication credentials.
- Multiple unspecified vulnerabilities.

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 Multiple Vulnerabilities (Apr 2016) - Linux
OID:1.3.6.1.4.1.25623.1.0.108388
Version used: 2024-02-20T14:37:13Z

References

```
cve: CVE-2016-0695
cve: CVE-2016-0687
cve: CVE-2016-0686
cve: CVE-2016-3443
cve: CVE-2016-3427
cve: CVE-2016-3425
cve: CVE-2016-3422
cve: CVE-2016-3449
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.ht
↪ml
cert-bund: WID-SEC-2023-1214
cert-bund: CB-K17/0796
cert-bund: CB-K17/0090
cert-bund: CB-K16/1080
cert-bund: CB-K16/0800
cert-bund: CB-K16/0726
cert-bund: CB-K16/0634
cert-bund: CB-K16/0594
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-0640
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Oct 2016) - Linux

Summary

Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote user to access and modify data on the target system, also can obtain elevated privileges on the target system.

Solution:

... continues on next page ...

. . . continued from previous page . . .

Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 121 and prior, 7 update 111 and prior, and 8 update 102 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to:
- A flaw in the 2D component.
- A flaw in the AWT component.
- A flaw in the Hotspot component.
- A flaw in the Networking component.
- A flaw in the JMX component.
- A flaw in the Libraries component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Oct 2016) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108385
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-5556
cve: CVE-2016-5568
cve: CVE-2016-5582
cve: CVE-2016-5573
cve: CVE-2016-5597
cve: CVE-2016-5554
cve: CVE-2016-5542
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
url: http://www.securityfocus.com/bid/93618
url: http://www.securityfocus.com/bid/93621
url: http://www.securityfocus.com/bid/93623
url: http://www.securityfocus.com/bid/93628
cert-bund: CB-K17/0895
cert-bund: CB-K17/0892
cert-bund: CB-K17/0874
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0456
cert-bund: CB-K17/0055
cert-bund: CB-K16/1802
cert-bund: CB-K16/1615
dfn-cert: DFN-CERT-2017-0921
dfn-cert: DFN-CERT-2017-0920
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0903
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0471
dfn-cert: DFN-CERT-2017-0060
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

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 Java SE version 1.6.0.151 and earlier, 1.7.0.141 and earlier, 1.8.0.131 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecifide errors in 'Security', 'AWT', 'ImageIO', 'JAXP', 'Libraries', 'RMI', 'Hotspot', 'JCE', 'JAX-WS', '2D', 'Serialization', 'Deployment' component of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108375
Version used: `2023-03-24T10:19:42Z`

References

```
cve: CVE-2017-10198
cve: CVE-2017-10096
cve: CVE-2017-10135
cve: CVE-2017-10110
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-10115
cve: CVE-2017-10116
cve: CVE-2017-10074
cve: CVE-2017-10053
cve: CVE-2017-10087
cve: CVE-2017-10089
cve: CVE-2017-10243
cve: CVE-2017-10102
cve: CVE-2017-10101
cve: CVE-2017-10107
cve: CVE-2017-10109
cve: CVE-2017-10105
cve: CVE-2017-10081
cve: CVE-2017-10193
cve: CVE-2017-10067
cve: CVE-2017-10108
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
url: http://www.securityfocus.com/bid/99818
url: http://www.securityfocus.com/bid/99670
url: http://www.securityfocus.com/bid/99839
url: http://www.securityfocus.com/bid/99643
url: http://www.securityfocus.com/bid/99774
url: http://www.securityfocus.com/bid/99734
url: http://www.securityfocus.com/bid/99731
url: http://www.securityfocus.com/bid/99842
url: http://www.securityfocus.com/bid/99703
url: http://www.securityfocus.com/bid/99659
url: http://www.securityfocus.com/bid/99827
url: http://www.securityfocus.com/bid/99712
url: http://www.securityfocus.com/bid/99674
url: http://www.securityfocus.com/bid/99719
url: http://www.securityfocus.com/bid/99847
url: http://www.securityfocus.com/bid/99851
url: http://www.securityfocus.com/bid/99853
url: http://www.securityfocus.com/bid/99854
url: http://www.securityfocus.com/bid/99756
url: http://www.securityfocus.com/bid/99846
cert-bund: CB-K18/0030
cert-bund: CB-K18/0015
cert-bund: CB-K17/2168
cert-bund: CB-K17/1699
cert-bund: CB-K17/1496
cert-bund: CB-K17/1477
cert-bund: CB-K17/1470
cert-bund: CB-K17/1375
cert-bund: CB-K17/1199
dfn-cert: DFN-CERT-2019-0618
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2018-0014
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1775
dfn-cert: DFN-CERT-2017-1561
dfn-cert: DFN-CERT-2017-1543
dfn-cert: DFN-CERT-2017-1536
dfn-cert: DFN-CERT-2017-1438
dfn-cert: DFN-CERT-2017-1241
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Oct 2016) - Linux

Summary
Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow remote user to access and modify data on the target system, also can obtain elevated privileges on the target system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 121 and prior, 7 update 111 and prior, and 8 update 102 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to:
- A flaw in the 2D component.
- A flaw in the AWT component.
- A flaw in the Hotspot component.
- A flaw in the Networking component.
- A flaw in the JMX component.
- A flaw in the Libraries 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 Java SE Multiple Unspecified Vulnerabilities-01 (Oct 2016) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108385
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-5556
cve: CVE-2016-5568
cve: CVE-2016-5582
cve: CVE-2016-5573
cve: CVE-2016-5597
cve: CVE-2016-5554
cve: CVE-2016-5542
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
url: http://www.securityfocus.com/bid/93618
url: http://www.securityfocus.com/bid/93621
url: http://www.securityfocus.com/bid/93623
url: http://www.securityfocus.com/bid/93628
cert-bund: CB-K17/0895
cert-bund: CB-K17/0892
cert-bund: CB-K17/0874
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0456
cert-bund: CB-K17/0055
cert-bund: CB-K16/1802
cert-bund: CB-K16/1615
dfn-cert: DFN-CERT-2017-0921
dfn-cert: DFN-CERT-2017-0920
dfn-cert: DFN-CERT-2017-0903
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0471
dfn-cert: DFN-CERT-2017-0060
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Vulnerabilities (Apr 2016) - Linux

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via different vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 113 and prior, 7 update 99 and prior and 8 update 77 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- The Security component in 'OpenJDK' failed to check the digest algorithm strength when generating DSA signatures.
- The JAXP component in 'OpenJDK' failed to properly handle Unicode surrogate pairs used as part of the XML attribute values.
- The RMI server implementation in the JMX component in 'OpenJDK' did not restrict which classes can be deserialized when deserializing authentication credentials.
- Multiple unspecified vulnerabilities.

Vulnerability Detection Method

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

Details: `Oracle Java SE Multiple Vulnerabilities (Apr 2016) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108388

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-0695
cve: CVE-2016-0687
cve: CVE-2016-0686
cve: CVE-2016-3443
cve: CVE-2016-3427
cve: CVE-2016-3425
cve: CVE-2016-3422
cve: CVE-2016-3449
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.ht
↪ml
cert-bund: WID-SEC-2023-1214
cert-bund: CB-K17/0796
cert-bund: CB-K17/0090
cert-bund: CB-K16/1080
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0800
cert-bund: CB-K16/0726
cert-bund: CB-K16/0634
cert-bund: CB-K16/0594
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-0640
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to gain elevated privileges, partially access and partially modify data, access sensitive data, obtain sensitive information or cause a denial of service, .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier, 9.0 on Linux.

Vulnerability Insight
Multiple flaws exist due to flaws in the 'Hotspot', 'RMI ', 'Libraries', 'Smart Card IO', 'Security', 'Javadoc', 'JAXP', 'Serialization' and 'Networking' components of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108379
Version used: `2022-08-01T10:11:45Z`

References

```
cve: CVE-2017-10388
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-10293
cve: CVE-2017-10346
cve: CVE-2017-10345
cve: CVE-2017-10285
cve: CVE-2017-10356
cve: CVE-2017-10348
cve: CVE-2017-10295
cve: CVE-2017-10349
cve: CVE-2017-10347
cve: CVE-2017-10274
cve: CVE-2017-10355
cve: CVE-2017-10357
cve: CVE-2017-10281
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101321
url: http://www.securityfocus.com/bid/101338
url: http://www.securityfocus.com/bid/101315
url: http://www.securityfocus.com/bid/101396
url: http://www.securityfocus.com/bid/101319
url: http://www.securityfocus.com/bid/101413
url: http://www.securityfocus.com/bid/101354
url: http://www.securityfocus.com/bid/101384
url: http://www.securityfocus.com/bid/101348
url: http://www.securityfocus.com/bid/101382
url: http://www.securityfocus.com/bid/101333
url: http://www.securityfocus.com/bid/101369
url: http://www.securityfocus.com/bid/101355
url: http://www.securityfocus.com/bid/101378
cert-bund: CB-K18/0715
cert-bund: CB-K18/0570
cert-bund: CB-K18/0495
cert-bund: CB-K18/0301
cert-bund: CB-K18/0030
cert-bund: CB-K17/2199
cert-bund: CB-K17/2168
cert-bund: CB-K17/2106
cert-bund: CB-K17/2047
cert-bund: CB-K17/1745
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0691
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0643
dfn-cert: DFN-CERT-2018-0536
dfn-cert: DFN-CERT-2018-0318
dfn-cert: DFN-CERT-2018-0039
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-2203
dfn-cert: DFN-CERT-2017-2135
dfn-cert: DFN-CERT-2017-1825
```

High (CVSS: 9.3)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2014) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow remote attackers to update, insert, or delete certain data, execute arbitrary code, conduct a denial of service and disclosure of potentially sensitive information.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 65 and prior, 6 update 75 and prior, 7 update 60 and prior, and 8 update 5 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist:
- An error in the JMX subcomponent related to share/classes/com/sun/jmx/remote/security/SubjectDelegator.java
- An error related to the Hotspot subcomponent in share/vm/classfile/classFileParser.hpp
- An error in the Libraries subcomponent related to share/classes/java/lang/reflect/Proxy.java and handling of interfaces passed to proxy methods.
- An error within the Swing subcomponent related to missing access restrictions imposed by the file choosers.
- An error in the Security subcomponent related to share/classes/java/security/Provider.java and instantiation of security services with non-public constructors.
- An error in the Diffie-Hellman key agreement within the Security subcomponent related to 'validateDHPublicKey' function in share/classes/sun/security/util/KeyUtil.java
- An error in Libraries subcomponent within 'AtomicReferenceFieldUpdaterImpl' function in /java/util/concurrent/atomic/AtomicReferenceFieldUpdater.java
- An error in the Security subcomponent related to share/classes/sun/security/rsa/RSACore.java and RSA 'blinding'.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108410
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-4244
cve: CVE-2014-4262
cve: CVE-2014-4263
cve: CVE-2014-4252
cve: CVE-2014-4268
cve: CVE-2014-4218
cve: CVE-2014-4216
cve: CVE-2014-4209
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68562
url: http://www.securityfocus.com/bid/68583
url: http://www.securityfocus.com/bid/68599
url: http://www.securityfocus.com/bid/68615
url: http://www.securityfocus.com/bid/68624
url: http://www.securityfocus.com/bid/68636
url: http://www.securityfocus.com/bid/68639
url: http://www.securityfocus.com/bid/68642
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 9.3)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2014) - Linux

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

. . . 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 update, insert, or delete certain data, execute arbitrary code, conduct a denial of service and disclosure of potentially sensitive information.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5 update 65 and prior, 6 update 75 and prior, 7 update 60 and prior, and 8 update 5 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist:

- An error in the JMX subcomponent related to share/classes/com/sun/jmx/remote/security/SubjectDelegator.java
- An error related to the Hotspot subcomponent in share/vm/classfile/classFileParser.hpp
- An error in the Libraries subcomponent related to share/classes/java/lang/reflect/Proxy.java and handling of interfaces passed to proxy methods.
- An error within the Swing subcomponent related to missing access restrictions imposed by the file choosers.
- An error in the Security subcomponent related to share/classes/java/security/Provider.java and instantiation of security services with non-public constructors.
- An error in the Diffie-Hellman key agreement within the Security subcomponent related to 'validateDHPublicKey' function in share/classes/sun/security/util/KeyUtil.java
- An error in Libraries subcomponent within 'AtomicReferenceFieldUpdaterImpl' function in /java/util/concurrent/atomic/AtomicReferenceFieldUpdater.java
- An error in the Security subcomponent related to share/classes/sun/security/rsa/RSACore.java and RSA 'blinding'.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2014) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108410

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-4244
cve: CVE-2014-4262
cve: CVE-2014-4263
cve: CVE-2014-4252
cve: CVE-2014-4268
cve: CVE-2014-4218
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-4216
cve: CVE-2014-4209
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68562
url: http://www.securityfocus.com/bid/68583
url: http://www.securityfocus.com/bid/68599
url: http://www.securityfocus.com/bid/68615
url: http://www.securityfocus.com/bid/68624
url: http://www.securityfocus.com/bid/68636
url: http://www.securityfocus.com/bid/68639
url: http://www.securityfocus.com/bid/68642
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 9.3)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2014) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow remote attackers to update, insert, or delete certain data, execute arbitrary code, conduct a denial of service and disclosure of potentially sensitive information.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Oracle Java SE 5 update 65 and prior, 6 update 75 and prior, 7 update 60 and prior, and 8 update 5 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist:
- An error in the JMX subcomponent related to share/classes/com/sun/jmx/remote/security/SubjectDelegator.java
- An error related to the Hotspot subcomponent in share/vm/classfile/classFileParser.hpp
- An error in the Libraries subcomponent related to share/classes/java/lang/reflect/Proxy.java and handling of interfaces passed to proxy methods.
- An error within the Swing subcomponent related to missing access restrictions imposed by the file choosers.
- An error in the Security subcomponent related to share/classes/java/security/Provider.java and instantiation of security services with non-public constructors.
- An error in the Diffie-Hellman key agreement within the Security subcomponent related to 'validateDHPublicKey' function in share/classes/sun/security/util/KeyUtil.java
- An error in Libraries subcomponent within 'AtomicReferenceFieldUpdaterImpl' function in /java/util/concurrent/atomic/AtomicReferenceFieldUpdater.java
- An error in the Security subcomponent related to share/classes/sun/security/rsa/RSACore.java and RSA 'blinding'.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jul 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108410
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-4244
cve: CVE-2014-4262
cve: CVE-2014-4263
cve: CVE-2014-4252
cve: CVE-2014-4268
cve: CVE-2014-4218
cve: CVE-2014-4216
cve: CVE-2014-4209
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68562
url: http://www.securityfocus.com/bid/68583
url: http://www.securityfocus.com/bid/68599
url: http://www.securityfocus.com/bid/68615
url: http://www.securityfocus.com/bid/68624
url: http://www.securityfocus.com/bid/68636
url: http://www.securityfocus.com/bid/68639
url: http://www.securityfocus.com/bid/68642
url: http://securitytracker.com/id?1030577
```

. . . continues on next page . . .

... continued from previous page ...

```
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

High (CVSS: 9.0)
NVT: Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux

Summary
Oracle Java SE is prone to a remote privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation will allow remote attackers to gain elevated privileges.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier on Linux

Vulnerability Insight
The flaw exists due to an unspecified error in 'Java DB' component.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux`

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.813681
Version used: `2022-08-17T10:11:15Z`

References

```
cve: CVE-2018-2938
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1405
```

High (CVSS: 9.0)
NVT: Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux

Summary
Oracle Java SE is prone to a remote privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow remote attackers to gain elevated privileges.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier on Linux

Vulnerability Insight
The flaw exists due to an unspecified error in 'Java DB' component.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813681
Version used: `2022-08-17T10:11:15Z`

References

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2018-2938
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1405
```

High (CVSS: 9.0)
NVT: Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux

Summary
Oracle Java SE is prone to a remote privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow remote attackers to gain elevated privileges.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier on Linux

Vulnerability Insight
The flaw exists due to an unspecified error in 'Java DB' component.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813681
Version used: `2022-08-17T10:11:15Z`

References

```
cve: CVE-2018-2938
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1405
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow attackers to cause some unspecified impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.141 and earlier, 1.7.0.131 and earlier, 1.8.0.121 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in 'AWT', 'JCE', 'JAXP', 'Networking', 'Security' and 'Deployment' sub-components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108382
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-3514
cve: CVE-2017-3526
cve: CVE-2017-3509
cve: CVE-2017-3533
cve: CVE-2017-3544
cve: CVE-2017-3539
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/97729
url: http://www.securityfocus.com/bid/97733
url: http://www.securityfocus.com/bid/97737
url: http://www.securityfocus.com/bid/97740
url: http://www.securityfocus.com/bid/97745
url: http://www.securityfocus.com/bid/97752
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
↪#AppendixJAVA
cert-bund: CB-K17/2168
cert-bund: CB-K17/1134
cert-bund: CB-K17/1133
cert-bund: CB-K17/0877
cert-bund: CB-K17/0784
cert-bund: CB-K17/0653
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2017-0676
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates-03 (cpuoct2018) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     See reference
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation will allow attackers to gain elevated privileges, cause partial denial of service conditions, partially modify and access data.

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

Affected Software/OS
Oracle Java SE version 1.6.0 through 1.6.0.201, 1.7.0 through 1.7.0.191, 1.8.0 through 1.8.0.181 and 11.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws are due to errors in components 'JNDI', 'Deployment (libpng)', 'Security', 'Networking' and 'JSSE'.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates-03 (cpuoct2018) - Linux`

OID:1.3.6.1.4.1.25623.1.0.814405

Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-3149
cve: CVE-2018-13785
cve: CVE-2018-3136
cve: CVE-2018-3139
cve: CVE-2018-3180
cve: CVE-2018-14048
url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixJAVA
advisory-id: cpuoct2018
cert-bund: CB-K19/1121
cert-bund: CB-K19/0175
cert-bund: CB-K19/0016
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2022-1175
dfn-cert: DFN-CERT-2020-0353
dfn-cert: DFN-CERT-2019-1110
dfn-cert: DFN-CERT-2019-0900
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0406
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2379
dfn-cert: DFN-CERT-2018-2107
dfn-cert: DFN-CERT-2018-1417
dfn-cert: DFN-CERT-2018-1361
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates-03 (cpuoct2018) - Linux

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     See reference
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow attackers to gain elevated privileges, cause partial denial of service conditions, partially modify and access data.

Solution:

Solution type: VendorFix

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

Affected Software/OS

Oracle Java SE version 1.6.0 through 1.6.0.201, 1.7.0 through 1.7.0.191, 1.8.0 through 1.8.0.181 and 11.

Vulnerability Insight

Multiple flaws are due to errors in components 'JNDI', 'Deployment (libpng)', 'Security', 'Networking' and 'JSSE'.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates-03 (cpuoct2018) - Linux`

OID:1.3.6.1.4.1.25623.1.0.814405

Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-3149
cve: CVE-2018-13785
cve: CVE-2018-3136
cve: CVE-2018-3139
cve: CVE-2018-3180
cve: CVE-2018-14048
url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixJAVA
advisory-id: cpuoct2018
cert-bund: CB-K19/1121
cert-bund: CB-K19/0175
cert-bund: CB-K19/0016
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2022-1175
dfn-cert: DFN-CERT-2020-0353
dfn-cert: DFN-CERT-2019-1110
dfn-cert: DFN-CERT-2019-0900
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0406
dfn-cert: DFN-CERT-2019-0076
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2379
dfn-cert: DFN-CERT-2018-2107
dfn-cert: DFN-CERT-2018-1417
dfn-cert: DFN-CERT-2018-1361
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates-03 (cpuoct2018) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     See reference
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow attackers to gain elevated privileges, cause partial denial of service conditions, partially modify and access data.

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

Affected Software/OS
Oracle Java SE version 1.6.0 through 1.6.0.201, 1.7.0 through 1.7.0.191, 1.8.0 through 1.8.0.181 and 11.

Vulnerability Insight
Multiple flaws are due to errors in components 'JNDI', 'Deployment (libpng)', 'Security', 'Networking' and 'JSSE'.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-03 (cpuoct2018) - Linux`
OID:1.3.6.1.4.1.25623.1.0.814405
Version used: `2023-11-03T16:10:08Z`

References

```
cve: CVE-2018-3149
cve: CVE-2018-13785
cve: CVE-2018-3136
cve: CVE-2018-3139
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-3180
cve: CVE-2018-14048
url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixJAVA
advisory-id: cpuoct2018
cert-bund: CB-K19/1121
cert-bund: CB-K19/0175
cert-bund: CB-K19/0016
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2022-1175
dfn-cert: DFN-CERT-2020-0353
dfn-cert: DFN-CERT-2019-1110
dfn-cert: DFN-CERT-2019-0900
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0406
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2379
dfn-cert: DFN-CERT-2018-2107
dfn-cert: DFN-CERT-2018-1417
dfn-cert: DFN-CERT-2018-1361
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial of service condition, access data, partially modify data and gain elevated privileges.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier, 9.0.1 and earlier on Linux.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws exist due to:
- Multiple errors in 'Libraries' sub-component.
- Multiple errors in 'JNDI' sub-component.
- An error in 'JMX' sub-component.
- Multiple errors in 'AWT' sub-component.
- An error in 'JCE' sub-component.
- An error in 'JGSS' sub-component.
- An error in 'I18n' sub-component.
- An error in 'LDAP' sub-component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108370
Version used: `2023-11-23T05:06:17Z`

References

```
cve: CVE-2018-2677
cve: CVE-2018-2599
cve: CVE-2018-2603
cve: CVE-2018-2641
cve: CVE-2018-2602
cve: CVE-2018-2629
cve: CVE-2018-2678
cve: CVE-2018-2663
cve: CVE-2018-2633
cve: CVE-2018-2588
cve: CVE-2018-2637
cve: CVE-2018-2618
cve: CVE-2018-2579
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0882
cert-bund: CB-K18/0808
cert-bund: CB-K18/0715
cert-bund: CB-K18/0714
cert-bund: CB-K18/0689
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1703
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-1073
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1000
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial of service condition, access data, partially modify data and gain elevated privileges.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier, 9.0.1 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors in 'Libraries' sub-component.
- Multiple errors in 'JNDI' sub-component.
- An error in 'JMX' sub-component.
- Multiple errors in 'AWT' sub-component.
- An error in 'JCE' sub-component.
- An error in 'JGSS' sub-component.
- An error in 'I18n' sub-component.
- An error in 'LDAP' sub-component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108370
Version used: `2023-11-23T05:06:17Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2018-2677
cve: CVE-2018-2599
cve: CVE-2018-2603
cve: CVE-2018-2641
cve: CVE-2018-2602
cve: CVE-2018-2629
cve: CVE-2018-2678
cve: CVE-2018-2663
cve: CVE-2018-2633
cve: CVE-2018-2588
cve: CVE-2018-2637
cve: CVE-2018-2618
cve: CVE-2018-2579
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0882
cert-bund: CB-K18/0808
cert-bund: CB-K18/0715
cert-bund: CB-K18/0714
cert-bund: CB-K18/0689
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1703
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-1073
dfn-cert: DFN-CERT-2018-1000
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial of service condition, access data, partially modify data and gain elevated privileges.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier, 9.0.1 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- Multiple errors in 'Libraries' sub-component.
- Multiple errors in 'JNDI' sub-component.
- An error in 'JMX' sub-component.
- Multiple errors in 'AWT' sub-component.
- An error in 'JCE' sub-component.
- An error in 'JGSS' sub-component.
- An error in 'I18n' sub-component.
- An error in 'LDAP' sub-component.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108370

Version used: `2023-11-23T05:06:17Z`

References

```
cve: CVE-2018-2677
cve: CVE-2018-2599
cve: CVE-2018-2603
cve: CVE-2018-2641
cve: CVE-2018-2602
cve: CVE-2018-2629
cve: CVE-2018-2678
cve: CVE-2018-2663
cve: CVE-2018-2633
cve: CVE-2018-2588
cve: CVE-2018-2637
cve: CVE-2018-2618
cve: CVE-2018-2579
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0882
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0808
cert-bund: CB-K18/0715
cert-bund: CB-K18/0714
cert-bund: CB-K18/0689
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1703
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-1073
dfn-cert: DFN-CERT-2018-1000
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.162 and earlier, 1.6.0.181 and earlier, 1.7.0.171 and earlier, 10.0 on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors in 'Hotspot', 'Security', 'AWT', 'JMX' and 'Serialization' Java SE 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 Updates (apr2018-3678067) 04 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813310
Version used: `2023-11-24T16:09:32Z`

References

```
cve: CVE-2018-2814
cve: CVE-2018-2798
cve: CVE-2018-2797
cve: CVE-2018-2795
cve: CVE-2018-2790
cve: CVE-2018-2794
cve: CVE-2018-2815
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Oracle Java SE version 1.8.0.162 and earlier, 1.6.0.181 and earlier, 1.7.0.171 and earlier, 10.0 on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors in 'Hotspot', 'Security', 'AWT', 'JMX' and 'Serialization' Java SE components

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813310
Version used: `2023-11-24T16:09:32Z`

References

```
cve: CVE-2018-2814
cve: CVE-2018-2798
cve: CVE-2018-2797
cve: CVE-2018-2795
cve: CVE-2018-2790
cve: CVE-2018-2794
cve: CVE-2018-2815
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.162 and earlier, 1.6.0.181 and earlier, 1.7.0.171 and earlier, 10.0 on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors in 'Hotspot', 'Security', 'AWT', 'JMX' and 'Serialization' Java SE components

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813310
Version used: `2023-11-24T16:09:32Z`

References
```
cve: CVE-2018-2814
cve: CVE-2018-2798
cve: CVE-2018-2797
cve: CVE-2018-2795
cve: CVE-2018-2790
cve: CVE-2018-2794
cve: CVE-2018-2815
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow attackers to cause some unspecified impacts.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.141 and earlier, 1.7.0.131 and earlier, 1.8.0.121 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to multiple unspecified errors in 'AWT', 'JCE', 'JAXP', 'Networking', 'Security' and 'Deployment' sub-components.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108382

Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-3514
cve: CVE-2017-3526
cve: CVE-2017-3509
cve: CVE-2017-3533
cve: CVE-2017-3544
cve: CVE-2017-3539
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97729
url: http://www.securityfocus.com/bid/97733
url: http://www.securityfocus.com/bid/97737
url: http://www.securityfocus.com/bid/97740
url: http://www.securityfocus.com/bid/97745
url: http://www.securityfocus.com/bid/97752
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
↪#AppendixJAVA
cert-bund: CB-K17/2168
cert-bund: CB-K17/1134
cert-bund: CB-K17/1133
cert-bund: CB-K17/0877
```

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K17/0784
cert-bund: CB-K17/0653
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2017-0676
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow attackers to cause some unspecified impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.141 and earlier, 1.7.0.131 and earlier, 1.8.0.121 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in 'AWT', 'JCE', 'JAXP', 'Networking', 'Security' and 'Deployment' sub-components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108382
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-3514
cve: CVE-2017-3526
cve: CVE-2017-3509
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2017-3533
cve: CVE-2017-3544
cve: CVE-2017-3539
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97729
url: http://www.securityfocus.com/bid/97733
url: http://www.securityfocus.com/bid/97737
url: http://www.securityfocus.com/bid/97740
url: http://www.securityfocus.com/bid/97745
url: http://www.securityfocus.com/bid/97752
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
↪#AppendixJAVA
cert-bund: CB-K17/2168
cert-bund: CB-K17/1134
cert-bund: CB-K17/1133
cert-bund: CB-K17/0877
cert-bund: CB-K17/0784
cert-bund: CB-K17/0653
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2017-0676
```

High (CVSS: 7.8)
NVT: Sudo Heap-Based Buffer Overflow Vulnerability (Baron Samedit) - Active Check

Summary
Sudo is prone to a heap-based buffer overflow dubbed ’Baron Samedit’.

Vulnerability Detection Result

```
Used command: sudoedit -s ’\’ ‘perl -e ’print "A" x 65536’‘
Result: sudoedit -s ’’ ‘perl -e ’print "A" x 65536’‘
Segmentation fault
]0;vagrant@metasploitable3-ub1404: ~vagrant@metasploitable3-ub1404:~$
```

Solution:
Solution type: VendorFix
Update to version 1.9.5p2 or later.

Affected Software/OS
All legacy versions from 1.8.2 to 1.8.31p2 and all stable versions from 1.9.0 to 1.9.5p1 in their default configuration.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Sudo is allowing privilege escalation to root via 'sudoedit -s' and a command-line argument that ends with a single backslash character.

Vulnerability Detection Method

Runs a specific SSH command after the login to the target which is known to trigger an error message on affected versions of Sudo.

Details: `Sudo Heap-Based Buffer Overflow Vulnerability (Baron Samedit) - Active Check`

OID:1.3.6.1.4.1.25623.1.0.117187

Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2021-3156
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://www.sudo.ws/stable.html#1.9.5p2
url: https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-h
↪eap-based-buffer-overflow-in-sudo-baron-samedit
cert-bund: WID-SEC-2023-0066
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-0623
cert-bund: CB-K22/0130
cert-bund: CB-K21/0161
cert-bund: CB-K21/0092
dfn-cert: DFN-CERT-2022-0224
```

High (CVSS: 7.7)

NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Jul 2016) - Linux

Summary

Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow remote user to access and modify data on the target system, can cause denial of service conditions on the target system, a remote or local user can obtain elevated privileges on the target system, also a local user can modify data on the target system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle Java SE 6 update 115 and prior, 7 update 101 and prior, and 8 update 92 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to:
- A flaw in the Hotspot component.
- A flaw in the Install component.
- A flaw in the JAXP component.
- A flaw in the CORBA component.
- A flaw in the Networking component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Jul 2016) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108384
Version used: `2024-02-20T14:37:13Z`

References
```
cve: CVE-2016-3458
cve: CVE-2016-3485
cve: CVE-2016-3500
cve: CVE-2016-3503
cve: CVE-2016-3508
cve: CVE-2016-3550
url: http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
url: http://www.securityfocus.com/bid/91945
url: http://www.securityfocus.com/bid/91996
url: http://www.securityfocus.com/bid/91972
url: http://www.securityfocus.com/bid/91951
cert-bund: CB-K16/1993
cert-bund: CB-K16/1935
cert-bund: CB-K16/1364
cert-bund: CB-K16/1363
cert-bund: CB-K16/1323
cert-bund: CB-K16/1308
cert-bund: CB-K16/1304
cert-bund: CB-K16/1251
cert-bund: CB-K16/1099
```

High (CVSS: 7.7)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Jul 2016) - Linux

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote user to access and modify data on the target system, can cause denial of service conditions on the target system, a remote or local user can obtain elevated privileges on the target system, also a local user can modify data on the target system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 115 and prior, 7 update 101 and prior, and 8 update 92 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to:

- A flaw in the Hotspot component.
- A flaw in the Install component.
- A flaw in the JAXP component.
- A flaw in the CORBA component.
- A flaw in the Networking component.

Vulnerability Detection Method

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

Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Jul 2016) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108384

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-3458
cve: CVE-2016-3485
cve: CVE-2016-3500
cve: CVE-2016-3503
cve: CVE-2016-3508
cve: CVE-2016-3550
url: http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
url: http://www.securityfocus.com/bid/91945
url: http://www.securityfocus.com/bid/91996
url: http://www.securityfocus.com/bid/91972
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/91951
cert-bund: CB-K16/1993
cert-bund: CB-K16/1935
cert-bund: CB-K16/1364
cert-bund: CB-K16/1363
cert-bund: CB-K16/1323
cert-bund: CB-K16/1308
cert-bund: CB-K16/1304
cert-bund: CB-K16/1251
cert-bund: CB-K16/1099
```

High (CVSS: 7.7)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 (Jul 2016) - Linux

Summary
Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow remote user to access and modify data on the target system, can cause denial of service conditions on the target system, a remote or local user can obtain elevated privileges on the target system, also a local user can modify data on the target system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 115 and prior, 7 update 101 and prior, and 8 update 92 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to:
- A flaw in the Hotspot component.
- A flaw in the Install component.
- A flaw in the JAXP component.
- A flaw in the CORBA component.
- A flaw in the Networking 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 Java SE Multiple Unspecified Vulnerabilities-01 (Jul 2016) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108384
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-3458
cve: CVE-2016-3485
cve: CVE-2016-3500
cve: CVE-2016-3503
cve: CVE-2016-3508
cve: CVE-2016-3550
url: http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
url: http://www.securityfocus.com/bid/91945
url: http://www.securityfocus.com/bid/91996
url: http://www.securityfocus.com/bid/91972
url: http://www.securityfocus.com/bid/91951
cert-bund: CB-K16/1993
cert-bund: CB-K16/1935
cert-bund: CB-K16/1364
cert-bund: CB-K16/1363
cert-bund: CB-K16/1323
cert-bund: CB-K16/1308
cert-bund: CB-K16/1304
cert-bund: CB-K16/1251
cert-bund: CB-K16/1099
```

High (CVSS: 7.6)
NVT: Oracle Java SE Privilege Escalation Vulnerability - Linux

Summary

Oracle Java SE JRE is prone to a privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via unknown vectors.

Solution:

Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle Java SE 6 update 111 and prior, 7 update 95 and prior, 8 update 71 and prior, and 8 update 72 and prior on Linux.

Vulnerability Insight
The flaw exists due to some unspecified error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Privilege Escalation Vulnerability - Linux`
OID:1.3.6.1.4.1.25623.1.0.108389
Version used: `2024-02-15T05:05:40Z`

References

```
cve: CVE-2016-0603
url: http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0603-28743
↪60.html
cert-bund: CB-K16/0197
```

High (CVSS: 7.6)
NVT: Oracle Java SE JRE Unspecified Code Execution Vulnerability (Apr 2015) - Linux

Summary
Oracle Java SE JRE is prone to an arbitrary code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to execute arbitrary code on affected system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 91 and prior, 7 update 76 and prior, 8 update 40 and prior on Linux.

Vulnerability Insight
The flaw is due to error related to the Deployment subcomponent.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

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

Details: `Oracle Java SE JRE Unspecified Code Execution Vulnerability (Apr 2015) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108404

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0458
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74141
cert-bund: CB-K15/1751
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 7.6)
NVT: Oracle Java SE Privilege Escalation Vulnerability - Linux

Summary

Oracle Java SE JRE is prone to a privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 111 and prior, 7 update 95 and prior, 8 update 71 and prior, and 8 update 72 and prior on Linux.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The flaw exists due to some unspecified error.

Vulnerability Detection Method

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

Details: `Oracle Java SE Privilege Escalation Vulnerability - Linux`

OID:1.3.6.1.4.1.25623.1.0.108389

Version used: `2024-02-15T05:05:40Z`

References

```
cve: CVE-2016-0603
url: http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0603-28743
↪60.html
cert-bund: CB-K16/0197
```

High (CVSS: 7.6)

NVT: Oracle Java SE Privilege Escalation Vulnerability - Linux

Summary

Oracle Java SE JRE is prone to a privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 111 and prior, 7 update 95 and prior, 8 update 71 and prior, and 8 update 72 and prior on Linux.

Vulnerability Insight

The flaw exists due to some 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: `Oracle Java SE Privilege Escalation Vulnerability - Linux`
OID:1.3.6.1.4.1.25623.1.0.108389
Version used: `2024-02-15T05:05:40Z`

References

```
cve: CVE-2016-0603
url: http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0603-28743
↪60.html
cert-bund: CB-K16/0197
```

High (CVSS: 7.6)
NVT: Oracle Java SE JRE Unspecified Code Execution Vulnerability (Apr 2015) - Linux

Summary

Oracle Java SE JRE is prone to an arbitrary code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to execute arbitrary code on affected system.

Solution:

Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 91 and prior, 7 update 76 and prior, 8 update 40 and prior on Linux.

Vulnerability Insight

The flaw is due to error related to the Deployment subcomponent.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Unspecified Code Execution Vulnerability (Apr 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108404
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0458
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74141
cert-bund: CB-K15/1751
cert-bund: CB-K15/0850
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 7.6)
NVT: Oracle Java SE JRE Unspecified Code Execution Vulnerability (Apr 2015) - Linux

Summary
Oracle Java SE JRE is prone to an arbitrary code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to execute arbitrary code on affected system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 91 and prior, 7 update 76 and prior, 8 update 40 and prior on Linux.

Vulnerability Insight
The flaw is due to error related to the Deployment subcomponent.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Unspecified Code Execution Vulnerability (Apr 2015) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108404
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2015-0458
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74141
cert-bund: CB-K15/1751
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux

Summary
Oracle Java SE is prone to a remote security vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.6.0.181 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier on Linux.

Vulnerability Insight
The flaw is due to an unspecified error in the 'Security' component of Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813307
Version used: `2022-10-10T10:12:14Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-2783
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: WID-SEC-2023-0531
cert-bund: CB-K18/0882
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1931
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0724
dfn-cert: DFN-CERT-2018-0102
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux

Summary
Oracle Java SE is prone to a remote security vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.6.0.181 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier on Linux.

Vulnerability Insight
The flaw is due to an unspecified error in the 'Security' component of Java SE.

. . . 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 Updates (apr2018-3678067) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.813307

Version used: `2022-10-10T10:12:14Z`

References

```
cve: CVE-2018-2783
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: WID-SEC-2023-0531
cert-bund: CB-K18/0882
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1931
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0724
dfn-cert: DFN-CERT-2018-0102
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux

Summary

Oracle Java SE is prone to a remote security vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

. . . continues on next page . . .

... continued from previous page ...

Affected Software/OS

Oracle Java SE version 1.6.0.181 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier on Linux.

Vulnerability Insight

The flaw is due to an unspecified error in the 'Security' component of Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813307
Version used: `2022-10-10T10:12:14Z`

References

```
cve: CVE-2018-2783
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: WID-SEC-2023-0531
cert-bund: CB-K18/0882
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1931
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0724
dfn-cert: DFN-CERT-2018-0102
```

[return to 192.168.56.105]

2.1.5 Medium 631/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

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
```

... continues on next page ...

... continued from previous page ...

```
↪ 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`

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
```

... continues on next page ...

. . . continued from previous page . . .

```
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
dfn-cert: DFN-CERT-2012-1377
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

[return to 192.168.56.105]

2.1.6 Medium 80/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.9.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       /phpmyadmin/js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.56.105/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://192.168.56.105/phpmyadmin/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.6.2
Fixed version:     1.9.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       /phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.56.105/phpmyadmin/setup/../js/jquery/jquery-1.
↪6.2.js
- Referenced at:   http://192.168.56.105/phpmyadmin/setup/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
The following input fields were identified (URL:input name):
http://192.168.56.105/drupal/:pass
http://192.168.56.105/drupal/?D=A:pass
http://192.168.56.105/payroll_app.php:password
http://192.168.56.105/phpmyadmin/:pma_password
http://192.168.56.105/phpmyadmin/?D=A:pma_password
http://192.168.56.105/phpmyadmin/changelog.php:pma_password
http://192.168.56.105/phpmyadmin/index.php:pma_password
http://192.168.56.105/phpmyadmin/license.php:pma_password
http://192.168.56.105/phpmyadmin/url.php:pma_password
```

Impact

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: jQuery < 1.6.3 XSS Vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /phpmyadmin/js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.56.105/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://192.168.56.105/phpmyadmin/
```

Solution:

Solution type: VendorFix

Update to version 1.6.3 or later.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Insight

Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method

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

Details: `jQuery < 1.6.3 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141637

Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
```

Medium (CVSS: 4.3)

NVT: jQuery < 1.6.3 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:       /phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.56.105/phpmyadmin/setup/../js/jquery/jquery-1.
↪6.2.js
- Referenced at:   http://192.168.56.105/phpmyadmin/setup/
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

References
```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
```

[return to 192.168.56.105]

2.1.7 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 Anonymous login ok, send your complete email address
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ as your password
```

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.

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 192.168.56.105]

2.1.8 Medium 22/tcp

Medium (CVSS: 5.3)

NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                         | Reason
--------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1  | Using SHA-1
diffie-hellman-group1-sha1          | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact

An attacker can quickly break individual connections.

Solution:

Solution type: Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

References
```
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5
```

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

Summary
The remote SSH server is configured to allow / support weak host key algorithm(s).

Vulnerability Detection Result
```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
--------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2024-06-14T05:05:48Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6
```

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary

The remote SSH server is configured to allow / support weak encryption algorithm(s).

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight

- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms

Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc8758
url: https://www.kb.cert.org/vuls/id/958563
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3
```

[return to 192.168.56.105]

2.1.9 Medium general/tcp

Medium (CVSS: 6.8)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Oct 2014) - Linux

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow attackers to bypass security restrictions, disclose sensitive information, manipulate certain data, conduct IP spoofing attacks or hijack a mutually authenticated session.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 71 and prior, 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux

Vulnerability Insight
Multiple flaws exist due to:
- An unspecified error in share/classes/javax/crypto/CipherInputStream.java script related to streaming of input cipher streams.
- An error in share/classes/java/util/ResourceBundle.java script related to property processing and handling of names.
- An error in the 'LogRecord::readObject' function in classes/java/util/logging/LogRecord.java related to handling of resource bundles.
- An error related to the wrapping of datagram sockets in the DatagramSocket implementation.
- An error in share/classes/java/util/logging/Logger.java related to missing permission checks of logger resources.
- An error related to handling of server certificate changes during SSL/TLS renegotiation.
- An error within the 2D subcomponent of the client deployment.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Oct 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108411
Version used: `2024-02-20T14:37:13Z`

References
```
cve: CVE-2014-6558
cve: CVE-2014-6531
cve: CVE-2014-6502
cve: CVE-2014-6512
cve: CVE-2014-6511
cve: CVE-2014-6506
cve: CVE-2014-6457
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70533
url: http://www.securityfocus.com/bid/70538
url: http://www.securityfocus.com/bid/70544
url: http://www.securityfocus.com/bid/70548
url: http://www.securityfocus.com/bid/70556
```

... continues on next page ...

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/70567
url: http://www.securityfocus.com/bid/70572
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

Medium (CVSS: 6.8)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Oct 2014) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow attackers to bypass security restrictions, disclose sensitive information, manipulate certain data, conduct IP spoofing attacks or hijack a mutually authenticated session.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 71 and prior, 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux

Vulnerability Insight
Multiple flaws exist due to:
- An unspecified error in share/classes/javax/crypto/CipherInputStream.java script related to streaming of input cipher streams.
- An error in share/classes/java/util/ResourceBundle.java script related to property processing and handling of names.
- An error in the 'LogRecord::readObject' function in classes/java/util/logging/LogRecord.java related to handling of resource bundles.
- An error related to the wrapping of datagram sockets in the DatagramSocket implementation.

. . . continues on next page . . .

. . . continued from previous page . . .

- An error in share/classes/java/util/logging/Logger.java related to missing permission checks of logger resources.
- An error related to handling of server certificate changes during SSL/TLS renegotiation.
- An error within the 2D subcomponent of the client deployment.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Oct 2014) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108411

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-6558
cve: CVE-2014-6531
cve: CVE-2014-6502
cve: CVE-2014-6512
cve: CVE-2014-6511
cve: CVE-2014-6506
cve: CVE-2014-6457
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70533
url: http://www.securityfocus.com/bid/70538
url: http://www.securityfocus.com/bid/70544
url: http://www.securityfocus.com/bid/70548
url: http://www.securityfocus.com/bid/70556
url: http://www.securityfocus.com/bid/70567
url: http://www.securityfocus.com/bid/70572
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

Medium (CVSS: 6.8)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Oct 2014) - Linux

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

. . . continues on next page . . .

... continued from previous page ...

Impact

Successful exploitation will allow attackers to bypass security restrictions, disclose sensitive information, manipulate certain data, conduct IP spoofing attacks or hijack a mutually authenticated session.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5 update 71 and prior, 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux

Vulnerability Insight

Multiple flaws exist due to:

- An unspecified error in share/classes/javax/crypto/CipherInputStream.java script related to streaming of input cipher streams.
- An error in share/classes/java/util/ResourceBundle.java script related to property processing and handling of names.
- An error in the 'LogRecord::readObject' function in classes/java/util/logging/LogRecord.java related to handling of resource bundles.
- An error related to the wrapping of datagram sockets in the DatagramSocket implementation.
- An error in share/classes/java/util/logging/Logger.java related to missing permission checks of logger resources.
- An error related to handling of server certificate changes during SSL/TLS renegotiation.
- An error within the 2D subcomponent of the client deployment.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Oct 2014) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108411

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-6558
cve: CVE-2014-6531
cve: CVE-2014-6502
cve: CVE-2014-6512
cve: CVE-2014-6511
cve: CVE-2014-6506
cve: CVE-2014-6457
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70533
url: http://www.securityfocus.com/bid/70538
url: http://www.securityfocus.com/bid/70544
```

... continues on next page ...

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/70548
url: http://www.securityfocus.com/bid/70556
url: http://www.securityfocus.com/bid/70567
url: http://www.securityfocus.com/bid/70572
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     1.9.0
Installation
path / port:       /opt/chef/embedded/lib/ruby/gems/2.4.0/gems/chef-13.8.5/distr
↪o/common/html/_static/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sdoc-0.4.1/lib/
↪rdoc/generator/template/sdoc/resources/js/jquery-1.3.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.4
Fixed version:     1.9.0
Installation
path / port:       /opt/chef/embedded/lib/ruby/2.4.0/rdoc/generator/template/dar
↪kfish/js/jquery.js
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: `2023-07-14T05:06:08Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.4
Fixed version:     1.9.0
Installation
path / port:       /usr/lib/ruby/1.9.1/rdoc/generator/template/darkfish/js/jquer
↪y.js
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.4.4
Fixed version:     1.9.0
Installation
path / port:       /var/www/html/drupal/misc/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.4
Fixed version:     1.9.0
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/rdoc-4.2.2/lib/
↪rdoc/generator/template/darkfish/js/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
```

. . . continues on next page . . .

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/rails-4.2.4/gui
↪des/assets/javascripts/jquery.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.9.0
Installation
path / port:       /opt/chef/embedded/lib/ruby/gems/2.4.0/gems/simplecov-html-0.
↪10.2/assets/javascripts/libraries/jquery-1.6.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.4
Fixed version:     1.9.0
Installation
path / port:       /opt/chef/embedded/lib/ruby/gems/2.4.0/gems/ruby-prof-0.17.0/
↪doc/js/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.9.0
Installation
path / port:       /var/www/html/phpmyadmin/js/jquery/jquery-1.6.2.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.7.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      1.9.0
Installation
path / port:        /usr/lib/ruby/2.3.0/rdoc/generator/template/darkfish/js/jquer
↪y.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        /usr/share/javascript/jquery/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sdoc-0.4.1/lib/
↪rdoc/generator/template/rails/resources/js/jquery-1.3.2.min.js
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
path / port:       /usr/share/javascript/jquery/jquery.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation will allow remote attackers to modify data, partially access data, cause partial denial of service conditions.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier and 10.0 through 10.0.1 on Linux

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors in components 'Libraries', 'JSSE' and 'Concurrency'.

Vulnerability Detection Method

Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813683
Version used: `2022-07-26T10:10:42Z`

References

```
cve: CVE-2018-2973
cve: CVE-2018-2940
cve: CVE-2018-2952
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K19/0354
cert-bund: CB-K18/1076
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1902
dfn-cert: DFN-CERT-2018-1691
dfn-cert: DFN-CERT-2018-1675
dfn-cert: DFN-CERT-2018-1456
dfn-cert: DFN-CERT-2018-1405
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jan 2016) - Linux

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 105, 7 update 91, 8 update 66 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jan 2016) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108393
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-0494
cve: CVE-2015-8126
cve: CVE-2016-0483
cve: CVE-2016-0402
cve: CVE-2016-0466
cve: CVE-2016-0448
cve: CVE-2015-7575
url: http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
cert-bund: WID-SEC-2023-0428
cert-bund: CB-K16/1842
cert-bund: CB-K16/1552
cert-bund: CB-K16/1201
cert-bund: CB-K16/1102
cert-bund: CB-K16/1080
cert-bund: CB-K16/0962
cert-bund: CB-K16/0509
cert-bund: CB-K16/0459
cert-bund: CB-K16/0446
cert-bund: CB-K16/0343
cert-bund: CB-K16/0327
cert-bund: CB-K16/0310
cert-bund: CB-K16/0262
cert-bund: CB-K16/0244
cert-bund: CB-K16/0089
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0065
cert-bund: CB-K16/0001
cert-bund: CB-K15/1876
cert-bund: CB-K15/1839
cert-bund: CB-K15/1810
cert-bund: CB-K15/1803
cert-bund: CB-K15/1695
cert-bund: CB-K15/1666
dfn-cert: DFN-CERT-2015-1984
dfn-cert: DFN-CERT-2015-1938
dfn-cert: DFN-CERT-2015-1907
dfn-cert: DFN-CERT-2015-1905
dfn-cert: DFN-CERT-2015-1789
dfn-cert: DFN-CERT-2015-1762
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jan 2016) - Linux

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 105, 7 update 91, 8 update 66 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jan 2016) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108393

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2024-02-20T14:37:13Z

References

cve: CVE-2016-0494
cve: CVE-2015-8126
cve: CVE-2016-0483
cve: CVE-2016-0402
cve: CVE-2016-0466
cve: CVE-2016-0448
cve: CVE-2015-7575
url: http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
cert-bund: WID-SEC-2023-0428
cert-bund: CB-K16/1842
cert-bund: CB-K16/1552
cert-bund: CB-K16/1201
cert-bund: CB-K16/1102
cert-bund: CB-K16/1080
cert-bund: CB-K16/0962
cert-bund: CB-K16/0509
cert-bund: CB-K16/0459
cert-bund: CB-K16/0446
cert-bund: CB-K16/0343
cert-bund: CB-K16/0327
cert-bund: CB-K16/0310
cert-bund: CB-K16/0262
cert-bund: CB-K16/0244
cert-bund: CB-K16/0089
cert-bund: CB-K16/0065
cert-bund: CB-K16/0001
cert-bund: CB-K15/1876
cert-bund: CB-K15/1839
cert-bund: CB-K15/1810
cert-bund: CB-K15/1803
cert-bund: CB-K15/1695
cert-bund: CB-K15/1666
dfn-cert: DFN-CERT-2015-1984
dfn-cert: DFN-CERT-2015-1938
dfn-cert: DFN-CERT-2015-1907
dfn-cert: DFN-CERT-2015-1905
dfn-cert: DFN-CERT-2015-1789
dfn-cert: DFN-CERT-2015-1762

Medium (CVSS: 5.9)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jan 2016) - Linux

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 105, 7 update 91, 8 update 66 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 (Jan 2016) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108393

Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2016-0494
cve: CVE-2015-8126
cve: CVE-2016-0483
cve: CVE-2016-0402
cve: CVE-2016-0466
cve: CVE-2016-0448
cve: CVE-2015-7575
url: http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
cert-bund: WID-SEC-2023-0428
cert-bund: CB-K16/1842
cert-bund: CB-K16/1552
cert-bund: CB-K16/1201
cert-bund: CB-K16/1102
cert-bund: CB-K16/1080
cert-bund: CB-K16/0962
cert-bund: CB-K16/0509
cert-bund: CB-K16/0459
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0446
cert-bund: CB-K16/0343
cert-bund: CB-K16/0327
cert-bund: CB-K16/0310
cert-bund: CB-K16/0262
cert-bund: CB-K16/0244
cert-bund: CB-K16/0089
cert-bund: CB-K16/0065
cert-bund: CB-K16/0001
cert-bund: CB-K15/1876
cert-bund: CB-K15/1839
cert-bund: CB-K15/1810
cert-bund: CB-K15/1803
cert-bund: CB-K15/1695
cert-bund: CB-K15/1666
dfn-cert: DFN-CERT-2015-1984
dfn-cert: DFN-CERT-2015-1938
dfn-cert: DFN-CERT-2015-1907
dfn-cert: DFN-CERT-2015-1905
dfn-cert: DFN-CERT-2015-1789
dfn-cert: DFN-CERT-2015-1762
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow remote attackers to modify data, partially access data, cause partial denial of service conditions.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier and 10.0 through 10.0.1 on Linux

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors in components 'Libraries', 'JSSE' and 'Concurrency'.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813683
Version used: `2022-07-26T10:10:42Z`

References

```
cve: CVE-2018-2973
cve: CVE-2018-2940
cve: CVE-2018-2952
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K19/0354
cert-bund: CB-K18/1076
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1902
dfn-cert: DFN-CERT-2018-1691
dfn-cert: DFN-CERT-2018-1675
dfn-cert: DFN-CERT-2018-1456
dfn-cert: DFN-CERT-2018-1405
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow remote attackers to modify data, partially access data, cause partial denial of service conditions.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier and 10.0 through 10.0.1 on Linux

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors in components 'Libraries', 'JSSE' and 'Concurrency'.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813683
Version used: `2022-07-26T10:10:42Z`

References

```
cve: CVE-2018-2973
cve: CVE-2018-2940
cve: CVE-2018-2952
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K19/0354
cert-bund: CB-K18/1076
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1902
dfn-cert: DFN-CERT-2018-1691
dfn-cert: DFN-CERT-2018-1675
dfn-cert: DFN-CERT-2018-1456
dfn-cert: DFN-CERT-2018-1405
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux

Summary
Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:       /usr/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier on Linux.

Vulnerability Insight

The flaw exists due to an error in the 'Serialization' sub-component of the application.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108368

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

References

```
cve: CVE-2018-2657
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0808
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 5.3)

NVT: Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux

Summary

Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier on Linux.

Vulnerability Insight
The flaw exists due to an error in the 'Serialization' sub-component of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108368
Version used: `2023-10-27T16:11:32Z`

References

```
cve: CVE-2018-2657
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0808
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux

Summary
Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

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
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier on Linux.

Vulnerability Insight
The flaw exists due to an error in the 'Serialization' sub-component of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108368
Version used: `2023-10-27T16:11:32Z`

References

```
cve: CVE-2018-2657
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0808
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Denial of Service Vulnerability (cpuoct2018) - Linux

Summary
Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation will allow attackers to cause partial denial of service conditions.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle Java SE version 1.6.0 to 1.6.0.201, 1.7.0 to 1.7.0.191, 1.8.0 to 1.8.0.182 on Linux.

Vulnerability Insight
The flaw is due to error in 'Sound' component.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Denial of Service Vulnerability (cpuoct2018) - Linux`
OID:1.3.6.1.4.1.25623.1.0.814408
Version used: `2024-02-26T14:36:40Z`

References

```
cve: CVE-2018-3214
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
cert-bund: CB-K19/0175
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2107
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Denial of Service Vulnerability (cpuoct2018) - Linux

Summary
Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation will allow attackers to cause partial denial of service conditions.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.6.0 to 1.6.0.201, 1.7.0 to 1.7.0.191, 1.8.0 to 1.8.0.182 on Linux.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
The flaw is due to error in 'Sound' component.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Denial of Service Vulnerability (cpuoct2018) - Linux`
OID:1.3.6.1.4.1.25623.1.0.814408
Version used: `2024-02-26T14:36:40Z`

References

```
cve: CVE-2018-3214
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
cert-bund: CB-K19/0175
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2107
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Denial of Service Vulnerability (cpuoct2018) - Linux

Summary
Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow attackers to cause partial denial of service conditions.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.6.0 to 1.6.0.201, 1.7.0 to 1.7.0.191, 1.8.0 to 1.8.0.182 on Linux.

Vulnerability Insight
The flaw is due to error in 'Sound' component.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Denial of Service Vulnerability (cpuoct2018) - Linux`
OID:1.3.6.1.4.1.25623.1.0.814408
Version used: `2024-02-26T14:36:40Z`

References

```
cve: CVE-2018-3214
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
cert-bund: CB-K19/0175
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2107
```

Medium (CVSS: 5.0)
NVT: Oracle Java SE JRE Unspecified Vulnerability-05 (Oct 2014) - Linux

Summary
Oracle Java SE JRE is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow attackers to disclose sensitive information.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5.0u71 and prior, 6u81 and prior, and 7u67 and prior on Linux.

Vulnerability Insight
The flaw exists due to an error related to C2 optimizations and range checks in the Hotspot subcomponent.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Unspecified Vulnerability-05 (Oct 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108426
Version used: `2024-02-20T14:37:13Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-6504
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70564
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
```

Medium (CVSS: 5.0)
NVT: Oracle Java SE JRE Unspecified Vulnerability-05 (Oct 2014) - Linux

Summary
Oracle Java SE JRE is prone to an unspecified vulnerability.

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

Impact
Successful exploitation will allow attackers to disclose sensitive information.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5.0u71 and prior, 6u81 and prior, and 7u67 and prior on Linux.

Vulnerability Insight
The flaw exists due to an error related to C2 optimizations and range checks in the Hotspot subcomponent.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Unspecified Vulnerability-05 (Oct 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108426
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-6504
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70564
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
```

Medium (CVSS: 5.0)
NVT: Oracle Java SE JRE Unspecified Vulnerability-05 (Oct 2014) - Linux

Summary
Oracle Java SE JRE is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact
Successful exploitation will allow attackers to disclose sensitive information.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5.0u71 and prior, 6u81 and prior, and 7u67 and prior on Linux.

Vulnerability Insight
The flaw exists due to an error related to C2 optimizations and range checks in the Hotspot subcomponent.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Unspecified Vulnerability-05 (Oct 2014) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108426
Version used: `2024-02-20T14:37:13Z`

References

```
cve: CVE-2014-6504
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70564
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sdoc-0.4.1/lib/
↪rdoc/generator/template/sdoc/resources/js/jquery-1.3.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.4.4
Fixed version:     1.6.3
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:       /var/www/html/drupal/misc/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

References
```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /opt/chef/embedded/lib/ruby/gems/2.4.0/gems/simplecov-html-0.
↪10.2/assets/javascripts/libraries/jquery-1.6.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

References
```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sdoc-0.4.1/lib/
↪rdoc/generator/template/rails/resources/js/jquery-1.3.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /var/www/html/phpmyadmin/js/jquery/jquery-1.6.2.js
```

Solution:

Solution type: VendorFix

Update to version 1.6.3 or later.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Insight

Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method

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

Details: `jQuery < 1.6.3 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141637

Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
```

Medium (CVSS: 4.2)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.162 and earlier, 1.7.0.171 and earlier, 1.6.0.181 and earlier on Linux.

Vulnerability Insight
The flaw is due to an unspecified error in 'RMI' component of Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813312
Version used: `2022-05-19T11:50:09Z`

References

```
cve: CVE-2018-2800
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

Medium (CVSS: 4.2)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.162 and earlier, 1.7.0.171 and earlier, 1.6.0.181 and earlier on Linux.

Vulnerability Insight

The flaw is due to an unspecified error in 'RMI' component of Java SE.

Vulnerability Detection Method

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

Details: Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux

OID:1.3.6.1.4.1.25623.1.0.813312

Version used: 2022-05-19T11:50:09Z

References

```
cve: CVE-2018-2800
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

Medium (CVSS: 4.2)

NVT: Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.162 and earlier, 1.7.0.171 and earlier, 1.6.0.181 and earlier on Linux.

Vulnerability Insight

The flaw is due to an unspecified error in 'RMI' component of Java SE.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux`

OID:1.3.6.1.4.1.25623.1.0.813312

Version used: `2022-05-19T11:50:09Z`

References

```
cve: CVE-2018-2800
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

[return to 192.168.56.105]

2.1.10 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary

The remote host responded to an ICMP timestamp request.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact

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 192.168.56.105]

2.1.11 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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):
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

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`

References

```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[return to 192.168.56.105]

2.1.12 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

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: 3351869
Packet 2: 3352135
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 192.168.56.105]

This file was automatically generated.