Scan Report

November 18, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "UTC", which is abbreviated "UTC". The task was "King-Arthur-Scan". The scan started at Mon Nov 18 18:41:26 2024 UTC and ended at Mon Nov 18 20:04:30 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.121.132 king-arthur	25	28	2	0	0
Total: 1	25	28	2	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 55 results selected by the filtering described above. Before filtering there were 146 results.

2 Results per Host

2.1 192.168.121.132

Host scan start	Mon Nov 18 18:42:04 2024 UTC
Host scan end	Mon Nov 18 20:04:24 2024 UTC

Service (Port)	Threat Level
3389/tcp	High
445/tcp	High
80/tcp	High
8022/tcp	High
8383/tcp	High
8019/tcp	High
8020/tcp	High
3050/tcp	High
135/tcp	Medium
3389/tcp	Medium
80/tcp	Medium
21/tcp	Medium
8443/tcp	Medium
8022/tcp	Medium
22/tcp	Medium

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
8383/tcp	Medium
8020/tcp	Medium
general/tcp	Low
general/icmp	Low

2.1.1 High 3389/tcp

High (CVSS: 9.8)
NVT: Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)

Summary
Microsoft Windows Remote Desktop Services is prone to the remote code execution vulnerability known as 'BlueKeep'.

Vulnerability Detection Result
```
By sending a crafted request the RDP service answered with a 'MCS Disconnect Pro
↪vider Ultimatum PDU - 2.2.2.3' response which indicates that a RCE attack can
↪be executed.
```

Impact
Successful exploitation would allow an attacker to execute arbitrary code on the target system. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.
As a workaround enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2.
NOTE: After enabling NLA affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.

Affected Software/OS
- Microsoft Windows 7
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2003
- Microsoft Windows Vista and Microsoft Windows XP (including Embedded)

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

A remote code execution vulnerability exists in Remote Desktop Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction.
For an in-depth analysis and further technical insights and details please see the references.

Vulnerability Detection Method
Sends a specially crafted request to the target systems Remote Desktop Service via RDP and checks the response.
Details: Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution.
↪..
OID:1.3.6.1.4.1.25623.1.0.108611
Version used: 2023-04-18T10:19:20Z

References
cve: CVE-2019-0708
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019
↪-0708
url: https://support.microsoft.com/help/4499164
url: https://support.microsoft.com/help/4499175
url: https://support.microsoft.com/help/4499149
url: https://support.microsoft.com/help/4499180
url: https://support.microsoft.com/help/4500331
url: https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updat
↪ing-remote-desktop-services-cve-2019-0708/
url: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-
↪2019-0708
url: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s
↪erver-2008-R2-and-2008/cc732713(v=ws.11)
url: http://www.securityfocus.com/bid/108273
url: http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Deskto
↪p-BlueKeep-Denial-Of-Service.html
url: https://www.malwaretech.com/2019/05/analysis-of-cve-2019-0708-bluekeep.html
url: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-
↪really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708
cert-bund: CB-K19/0415
dfn-cert: DFN-CERT-2019-0977

[return to 192.168.121.132]

2.1.2 High 445/tcp

High (CVSS: 8.1)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

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

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `2023-07-14T16:09:27Z`

References
`cve: CVE-2017-0143`
`cve: CVE-2017-0144`
`cve: CVE-2017-0145`
`cve: CVE-2017-0146`
`cve: CVE-2017-0147`
`cve: CVE-2017-0148`
`cisa: Known Exploited Vulnerability (KEV) catalog`

... continues on next page ...

... continued from previous page ...

```
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013078
url: http://www.securityfocus.com/bid/96703
url: http://www.securityfocus.com/bid/96704
url: http://www.securityfocus.com/bid/96705
url: http://www.securityfocus.com/bid/96707
url: http://www.securityfocus.com/bid/96709
url: http://www.securityfocus.com/bid/96706
url: https://technet.microsoft.com/library/security/MS17-010
url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448
```

[return to 192.168.121.132]

2.1.3 High 80/tcp

High (CVSS: 10.0)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)

Product detection result
cpe:/a:microsoft:internet_information_services:7.5
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: ↪ 1.3.6.1.4.1.25623.1.0.900710)

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

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

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

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

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

... continues on next page ...

... continued from previous page ...

- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

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

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response
Details: `MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)`
OID:1.3.6.1.4.1.25623.1.0.105257
Version used: `2023-07-25T05:05:58Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:7.5`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
`cve: CVE-2015-1635`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: https://support.microsoft.com/kb/3042553`
`url: https://technet.microsoft.com/library/security/MS15-034`
`url: http://pastebin.com/ypURDPc4`
`cert-bund: CB-K15/0527`
`dfn-cert: DFN-CERT-2015-0545`

[return to 192.168.121.132]

2.1.4 High 8022/tcp

High (CVSS: 10.0)
NVT: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability

Summary
ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

Vulnerability Detection Result
```
Installed version: 9.1.051
Fixed version:     10.0.082
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: /

Solution:
Solution type: VendorFix
Update to version 10.0.082 or later.

Affected Software/OS
ManageEngine Desktop Central before version 10.0.082.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vuln.
↪..
OID:1.3.6.1.4.1.25623.1.0.106809
Version used: 2021-09-23T03:58:52Z

References
cve: CVE-2017-7213
url: https://www.manageengine.com/products/desktop-central/cve-2017-7213-remote-
↪control-privilege-violation.html

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability

Summary
ManageEngine Desktop Central allows remote attackers to execute arbitrary code via vectors involving the upload of help desk videos.

Vulnerability Detection Result
Installed version: 9.1.051
Fixed version: 10.0.092
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 10.0.092 or later.

Affected Software/OS
ManageEngine Desktop Central before version 10.0.092.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.106969
Version used: 2021-09-23T03:58:52Z

References
cve: CVE-2017-11346
url: https://www.manageengine.com/products/desktop-central/remote-code-execution.html

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerability

Summary
ManageEngine Desktop Central 9 suffers from a vulnerability that allows a remote attacker to upload a malicious file, and execute it under the context of SYSTEM.

Vulnerability Detection Result
It was possible to upload the file 'http://king-arthur:8022/jspf/OpenVASVT_CVE-2015-8249_test.jsp'. Please delete this file.

Impact
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

Solution:
Solution type: VendorFix
Update to version 9.0.142 or later.

Affected Software/OS
ManageEngine Desktop Central prior to version 9.0.142.

Vulnerability Detection Method
Try to upload a jsp file.
Details: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerabi..
OID:1.3.6.1.4.1.25623.1.0.140041
Version used: 2021-10-12T12:01:25Z

References
cve: CVE-2015-8249

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

ManageEngine Desktop Central is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 9.1.051
Fixed version:     10.0.157
Installation
path / port:       /
```

Impact

Successful exploitation will allow attacker to download unencrypted XML files containing all data for configuration policies.

Solution:

Solution type: VendorFix

Update to version 10.0.157 or later.

Affected Software/OS

ManageEngine Desktop Central/MSP version 10.0.137 and prior.

Vulnerability Insight

This issue exists in an unknown function of the file '/client-data//collections/##/usermgmt.xml'.

Vulnerability Detection Method

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

Details: `ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure ..`

OID:1.3.6.1.4.1.25623.1.0.812522

Version used: `2023-01-19T10:10:48Z`

References

```
cve: CVE-2017-16924
url: https://www.manageengine.com/desktop-management-msp/password-encryption-policy-violation.html
```

High (CVSS: 9.8)

NVT: ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities

Summary

ManageEngine Desktop Central is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Vulnerable URL: http://king-arthur:8022/jsp/admin/DBQueryExecutor.jsp?actionFrom=getResult&query=SELECT%20*%20from%20aaauser;
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to write arbitrary files, gain access to unrestricted resources and execute remote code.

Solution:
Solution type: VendorFix
Update to version 10.0.208 or later.

Affected Software/OS
ManageEngine Desktop Central version 10.0.184 and prior.

Vulnerability Insight
Multiple flaws are due to:
- The missing authentication/authorization on a database query mechanism.
- An insufficient enforcement of database query type restrictions.
- The missing server side check on file type/extension when uploading and modifying scripts
- The directory traversal in SCRIPT_NAME field when modifying existing scripts

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.813213
Version used: `2021-09-23T03:58:52Z`

References
`cve: CVE-2018-5337`
`cve: CVE-2018-5338`
`cve: CVE-2018-5339`
`cve: CVE-2018-5341`
`url: https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vuln`
`↪erabilities-in-manageengine-desktop-central`

[return to 192.168.121.132]

2.1.5 High 8383/tcp

High (CVSS: 10.0)
NVT: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability

Summary
ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 9.1.051
Fixed version:     10.0.082
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 10.0.082 or later.

Affected Software/OS
ManageEngine Desktop Central before version 10.0.082.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vuln.
↪..`
OID:1.3.6.1.4.1.25623.1.0.106809
Version used: `2021-09-23T03:58:52Z`

References
`cve: CVE-2017-7213`
`url: https://www.manageengine.com/products/desktop-central/cve-2017-7213-remote-
↪control-privilege-violation.html`

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability

Summary
ManageEngine Desktop Central allows remote attackers to execute arbitrary code via vectors involving the upload of help desk videos.

Vulnerability Detection Result

```
Installed version: 9.1.051
Fixed version:     10.0.092
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 10.0.092 or later.

Affected Software/OS
ManageEngine Desktop Central before version 10.0.092.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.092 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106969
Version used: `2021-09-23T03:58:52Z`

References
`cve: CVE-2017-11346`
`url: https://www.manageengine.com/products/desktop-central/remote-code-execution.html`

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities

Summary
ManageEngine Desktop Central is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Vulnerable URL: https://king-arthur:8383/jsp/admin/DBQueryExecutor.jsp?actionFrom=getResult&query=SELECT%20*%20from%20aaauser;`

Impact
Successful exploitation will allow attackers to write arbitrary files, gain access to unrestricted resources and execute remote code.

Solution:
Solution type: VendorFix
Update to version 10.0.208 or later.

Affected Software/OS
ManageEngine Desktop Central version 10.0.184 and prior.

Vulnerability Insight
Multiple flaws are due to:
- The missing authentication/authorization on a database query mechanism.
- An insufficient enforcement of database query type restrictions.
- The missing server side check on file type/extension when uploading and modifying scripts
- The directory traversal in SCRIPT_NAME field when modifying existing scripts

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.813213
Version used: `2021-09-23T03:58:52Z`

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2018-5337
cve: CVE-2018-5338
cve: CVE-2018-5339
cve: CVE-2018-5341
url: https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vuln
↪erabilities-in-manageengine-desktop-central

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerability

Summary
ManageEngine Desktop Central 9 suffers from a vulnerability that allows a remote attacker to upload a malicious file, and execute it under the context of SYSTEM.

Vulnerability Detection Result
It was possible to upload the file 'https://king-arthur:8383/jspf/OpenVASVT_CVE-
↪2015-8249_test.jsp'. Please delete this file.

Impact
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

Solution:
Solution type: VendorFix
Update to version 9.0.142 or later.

Affected Software/OS
ManageEngine Desktop Central prior to version 9.0.142.

Vulnerability Detection Method
Try to upload a jsp file.
Details: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerabi.
↪..
OID:1.3.6.1.4.1.25623.1.0.140041
Version used: 2021-10-12T12:01:25Z

References
cve: CVE-2015-8249

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

ManageEngine Desktop Central is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 9.1.051
Fixed version:     10.0.157
Installation
path / port:       /
```

Impact

Successful exploitation will allow attacker to download unencrypted XML files containing all data for configuration policies.

Solution:

Solution type: VendorFix

Update to version 10.0.157 or later.

Affected Software/OS

ManageEngine Desktop Central/MSP version 10.0.137 and prior.

Vulnerability Insight

This issue exists in an unknown function of the file '/client-data//collections/##/usermgmt.xml'.

Vulnerability Detection Method

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

Details: `ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure . ↪..`

OID:1.3.6.1.4.1.25623.1.0.812522

Version used: `2023-01-19T10:10:48Z`

References

```
cve: CVE-2017-16924
url: https://www.manageengine.com/desktop-management-msp/password-encryption-pol
↪icy-violation.html
```

High (CVSS: 9.8)

NVT: ManageEngine Desktop Central < 8.0.293 Arbitrary File Upload Vulnerability

Summary

ManageEngine Desktop Central is prone to an arbitrary file upload vulnerability.

Vulnerability Detection Result

```
It was possible to upload the file "/openvasvt123110615.jsp". Please delete this
↪ file.
Vulnerable URL: https://king-arthur:8383/agentLogUploader?computerName=DesktopCe
```

... continues on next page ...

... continued from previous page ...

↪ntral&domainName=webapps&customerId=1&filename=openvasvt123110615.jsp

Impact
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

Solution:
Solution type: VendorFix
Update to version 8.0.293 or later.

Affected Software/OS
ManageEngine Desktop Central prior to version 8.0.293.

Vulnerability Insight
The flaw in the AgentLogUploadServlet. This servlet takes input from HTTP POST and constructs an output file on the server without performing any sanitisation or even checking if the caller is authenticated.

Vulnerability Detection Method
Sends a crafted HTTP POST request and checks the response.
Details: ManageEngine Desktop Central < 8.0.293 Arbitrary File Upload Vulnerability
OID:1.3.6.1.4.1.25623.1.0.803777
Version used: 2021-10-15T09:03:25Z

References
cve: CVE-2013-7390
cve: CVE-2014-5007
url: http://www.exploit-db.com/exploits/29674
url: http://security-assessment.com/files/documents/advisory/DesktopCentral%20Ar
↪bitrary%20File%20Upload.pdf

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_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2023-07-20T05:05:17Z

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-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750

... continues on next page ...

... continued from previous page ...

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-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
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

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378

High (CVSS: 7.5)
NVT: '/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable URL: https://king-arthur:8383/.//WEB-INF/web.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

... continues on next page ...

... continued from previous page ...

Impact
Based on the information provided in this file an attacker might be able to gather additional info and/or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
The following vendor fixes are known:
- Update to Payara Platform Enterprise 5.31.0, Payara Platform Community 5.2021.7 or later.
For other products please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- Payara Platform Enterprise / Community
Other products might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/.//WEB-INF/web.xml
http://example.com/.//web-inf/web.xml
(note the './/' before 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117707
Version used: `2023-03-06T10:19:58Z`

References
`cve: CVE-2021-41381`
`url: https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-`
`↪054.txt`
`url: http://packetstormsecurity.com/files/164365/Payara-Micro-Community-5.2021.6`
`↪-Directory-Traversal.html`

[return to 192.168.121.132]

2.1.6 High 8019/tcp

High (CVSS: 9.8)
NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

Summary
Apache Tomcat is prone to a remote code execution vulnerability (dubbed 'Ghostcat') in the AJP connector.

Vulnerability Detection Result

```
It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.
Result:
AB Â¶\x0004 Ã\x0088 \x0002OK  \x0005
Accept-Ranges  \x0005bytes  \x0004ETag  \x0018W/"471636-1437727186000"
Last-Modified  \x001DFri, 24 Jul 2015 08:39:46 GMT  \x000CContent-Type  \x0016te
↪xt/xml;charset=UTF-8  \x000EContent-Length  \x0006471636 AB\x001FÃ¼\x0003\x001
↪FÃ¸<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
```

... continues on next page ...

... continued from previous page ...

```
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integration -->

 <filter>
         <filter-name>Security_Filter</filter-name>
         <filter-class>com.adventnet.iam.security.SecurityFilter</filter-class>
         <init-param>
             <param-name>config-file</param-name>
             <param-value>security-properties.xml,security-common.xml,security.x
↪ml</param-value>
         </init-param>
         <init-param>
             <param-name>development.mode</param-name>
             <param-value>false</param-value>
         </init-param>
         <init-param>
             <param-name>exclude</param-name>
             <param-value>/.*</param-value>
         </init-param>
     </filter>
     <filter-mapping>
         <filter-name>Security_Filter</filter-name>
         <url-pattern>/.*</url-pattern>
     </filter-mapping>

  <filter>
         <filter-name>DCXSSFilter</filter-name>
  <filter-class>com.adventnet.sym.webclient.xss.DCXSSFilter</filter-class>
↪

         <init-param>
             <param-name>exclude</param-name>
             <param-value>/.*\.js|/.*\.css|/.*\.txt|/.*\.html|/.*\.ico|/.*\.gif|
↪/.*\.jpg|/.*\.png|/.*\.xml</param-value>
         </init-param>
     </filter>
     <filter-mapping>
         <filter-name>DCXSSFilter</filter-name>
```

... continues on next page ...

... continued from previous page ...

```
          <url-pattern>/*</url-pattern>
      </filter-mapping>

  <!-- Added for RAD Development -->
  <filter>
  <filter-name>StateFilter</filter-name>
  <filter-class>com.adventnet.client.view.web.StateFilter</filter-class>
  </filter>
  <filter-mapping>
  <filter-name>StateFilter</filter-name>
  <url-pattern>/STATE_ID/*</url-pattern>
  </filter-mapping>
  <!-- Ended for RAD Development -->
  <filter>
  <filter-name>URLRedirectionFilter</filter-name>
  <filter-class>com.adventnet.sym.webclient.filter.URLRedirectionFilter</filter-
↪class>
  </filter>
  <filter-mapping>
  <filter-name>URLRedirectionFilter</filter-name>
  <url-pattern>/client-data/*</url-pattern>
  </filter-mapping>
  <filter-mapping>
  <filter-name>URLRedirectionFilter</filter-name>
  <url-pattern>/agent/*</url-pattern>
  </filter-mapping>
  <!-- MSP Specific Filter-->
  <filter>
  <filter-name>MSPCustomerFilter</filter-name>
  <filter-class>com.me.devicemanagement.framework.webclient.filter.MSPCustomerFi
↪lter</filter-class>
  </filter>
  <filter-mapping>
  <filter-name>MSPCustomerFilter</filter-name>
  <url-pattern>/*</url-pattern>
  <dispatcher>FORWARD</dispatcher>
  <dispatcher>REQUEST</dispatcher>
  </filter-mapping>

  <filter>
  <filter-name>UIRestrictionFilter</filter-name>
  <filter-class>com.adventnet.sym.webclient.filter.UIRestrictionFilter</filter-c
↪lass>
  </filter>
  <filter-mapping>
  <filter-name>UIRestrictionFilter</filter-name>
  <url-pattern>*.do</url-pattern>
```

... continues on next page ...

... continued from previous page ...

```
 <dispatcher>FORWARD</dispatcher>
 <dispatcher>REQUEST</dispatcher>
 <dispatcher>INCLUDE</dispatcher>
 <dispatcher>ERROR</dispatcher>
 </filter-mapping>
 <filter>
 <filter-name>DCAuthorizationFilter</filter-name>
 <filter-class>com.adventnet.sym.webclient.filter.DCAuthorizationFilter</filter
↪-class>
 </filter>
 <filter-mapping>
 <filter-name>DCAuthorizationFilter</filter-name>
 <url-pattern>*.do</url-pattern>
 </filter-mapping>
        <filter>
 <filter-name>LicenseFilter</filter-name>
 <filter-class>com.me.devicemanagement.framework.webclient.filter.LicenseFilter
↪</filter-class>
 </filter>

 <filter-mapping>
 <filter-name>LicenseFilter</filter-name>
 <url-pattern>/mdmTab.do</url-pattern>
 <url-pattern>/mdmAgentSettings.do</url-pattern>
 <url-pattern>/mdmLocation.do</url-pattern>
 <url-pattern>/mdmEnroll.do</url-pattern>
 <url-pattern>/mdmCustomDeviceDetails.do</url-pattern>
 <url-pattern>/mdmapns.do</url-pattern>
 <url-pattern>/mdmWPAppRepSettings.do</url-pattern>
 <url-pattern>/mdmWPAET.do</url-pattern>
 <url-pattern>/mdmEnrollSettings.do</url-pattern>
 <url-pattern>/mdmAppleConfig.do</url-pattern>
 <url-pattern>/mdmAuthentication.do</url-pattern>
 <url-pattern>/mdmBulkEnroll.do</url-pattern>
 <url-pattern>/mdmInv.do</url-pattern>
 <url-pattern>/mdmApp.do</url-pattern>
 <url-pattern>/mdmDeviceDetails.do</url-pattern>
 <url-pattern>/mdmInvDeviceScan.do</url-pattern>
 <url-pattern>/adminEmail.do</url-pattern>
 <url-pattern>/mdmReports.do</url-pattern>
 <url-pattern>/deviceMgmt.do</url-pattern>
 <url-pattern>/vppMgmt.do</url-pattern>
 <url-pattern>/appMgmt.do</url-pattern>
 <url-pattern>/appMgmtSource.do</url-pattern>
 <url-pattern>/addMoreLicense.do</url-pattern>
 <url-pattern>/appMgmtCatalogue.do</url-pattern>
 <url-pattern>/profileAudit.do</url-pattern>
```

... continues on next page ...

... continued from previous page ...

```
 <url-pattern>/profileMgmt.do</url-pattern>
 <url-pattern>/credentialMgmt.do</url-pattern>
 <url-pattern>/createProfile.do</url-pattern>
 <url-pattern>/viewProfile.do</url-pattern>
 <url-pattern>/mdmGroup.do</url-pattern>
 </filter-mapping>
  <filter>
                <filter-name>EncodingFilter</filter-name>
                <filter-class>com.adventnet.sym.webclient.filter.EncodingFilter
↪</filter-class>
         </filter>

         <filter-mapping>
                <filter-name>EncodingFilter</filter-name>
                <url-pattern>/*</url-pattern>
                <dispatcher>FORWARD</dispatcher>
                <dispatcher>REQUEST</dispatcher>
         </filter-mapping>

 <filter>
 <filter-name>MDMI18NLocaleFilter</filter-name>
        <filter-class>com.adventnet.sym.webclient.mdm.enroll.MDMI18NLocaleFilter
↪</filter-class>
    </filter>
   <filter-mapping>
 <filter-name>MDMI18NLocaleFilter</filter-name>
 <url-pattern>/mdm/enroll</url-pattern>
 <url-pattern>*.mob</url-pattern>
 <url-pattern>*.mobapps</url-pattern>
 <url-pattern>/mdm/apps</url-pattern>
 <url-pattern>/mdm/ios/acs</url-pattern>
 </filter-mapping>

 <!-- SDP-DC integration -->
 <servlet>
 <servlet-name>DCRequestHandler</servlet-name>
 <servlet-class>com.adventnet.sym.webclient.sdp.DCRequestHandler</servlet-class
↪>
 </servlet>
     <servlet-mapping>
 <servlet-name>DCRequestHandler</servlet-name>
 <url-pattern>/servlets/DCPluginServelet</url-pattern>
 </servlet-mapping>

 <servlet>
 <servlet-name>SDPDCRequestHandler</servlet-name>
 <servlet-class>com.adventnet.sym.webclient.sdp.SDPDCRequestHandler</servlet-cl
```

... continues on next page ...

... continued from previous page ...

```
↪ass>
 </servlet>
     <servlet-mapping>
 <servlet-name>SDPDCRequestHandler</servlet-name>
 <url-pattern>/DCRequestServlet</url-pattern>
 </servlet-mapping>

 <!--SDP-DC integration -->
 <!-- Li
```

Solution:
Solution type: VendorFix
Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on fixed versions.

Affected Software/OS
Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled.
Other products like JBoss or Wildfly which are using Tomcat might be affected as well.

Vulnerability Insight
Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.

Vulnerability Detection Method
Sends a crafted AJP request and checks the response.
Details: `Apache Tomcat AJP RCE Vulnerability (Ghostcat)`
OID:1.3.6.1.4.1.25623.1.0.143545
Version used: `2023-07-06T05:05:36Z`

References

```
cve: CVE-2020-1938
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1
↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
url: https://www.chaitin.cn/en/ghostcat
url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487
url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi
url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances
↪-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/
url: https://tomcat.apache.org/tomcat-7.0-doc/changelog.html
url: https://tomcat.apache.org/tomcat-8.5-doc/changelog.html
url: https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
cert-bund: CB-K20/0711
cert-bund: CB-K20/0705
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/0693
cert-bund: CB-K20/0555
cert-bund: CB-K20/0543
cert-bund: CB-K20/0154
dfn-cert: DFN-CERT-2021-1736
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-1413
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2020-1134
dfn-cert: DFN-CERT-2020-0850
dfn-cert: DFN-CERT-2020-0835
dfn-cert: DFN-CERT-2020-0821
dfn-cert: DFN-CERT-2020-0569
dfn-cert: DFN-CERT-2020-0557
dfn-cert: DFN-CERT-2020-0501
dfn-cert: DFN-CERT-2020-0381
```

[return to 192.168.121.132]

2.1.7 High 8020/tcp

High (CVSS: 10.0)
NVT: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability

Summary
ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

Vulnerability Detection Result

```
Installed version: 9.1.051
Fixed version:     10.0.082
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 10.0.082 or later.

Affected Software/OS
ManageEngine Desktop Central before version 10.0.082.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vuln.`

... continues on next page ...

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.106809
Version used: 2021-09-23T03:58:52Z

References
cve: CVE-2017-7213
url: https://www.manageengine.com/products/desktop-central/cve-2017-7213-remote-
↪control-privilege-violation.html

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability

Summary
ManageEngine Desktop Central allows remote attackers to execute arbitrary code via vectors involving the upload of help desk videos.

Vulnerability Detection Result
Installed version: 9.1.051
Fixed version: 10.0.092
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 10.0.092 or later.

Affected Software/OS
ManageEngine Desktop Central before version 10.0.092.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106969
Version used: 2021-09-23T03:58:52Z

References
cve: CVE-2017-11346
url: https://www.manageengine.com/products/desktop-central/remote-code-execution
↪.html

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure Vulnerability

... continues on next page ...

... continued from previous page ...

Summary
ManageEngine Desktop Central is prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 9.1.051
Fixed version:     10.0.157
Installation
path / port:       /
```

Impact
Successful exploitation will allow attacker to download unencrypted XML files containing all data for configuration policies.

Solution:
Solution type: VendorFix
Update to version 10.0.157 or later.

Affected Software/OS
ManageEngine Desktop Central/MSP version 10.0.137 and prior.

Vulnerability Insight
This issue exists in an unknown function of the file '/client-data//collections/##/usermgmt.xml'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.812522
Version used: `2023-01-19T10:10:48Z`

References
```
cve: CVE-2017-16924
url: https://www.manageengine.com/desktop-management-msp/password-encryption-pol
↪icy-violation.html
```

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities

Summary
ManageEngine Desktop Central is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Vulnerable URL: http://king-arthur:8020/jsp/admin/DBQueryExecutor.jsp?actionFrom
↪=getResult&query=SELECT%20*%20from%20aaauser;
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to write arbitrary files, gain access to unrestricted resources and execute remote code.

Solution:
Solution type: VendorFix
Update to version 10.0.208 or later.

Affected Software/OS
ManageEngine Desktop Central version 10.0.184 and prior.

Vulnerability Insight
Multiple flaws are due to:
- The missing authentication/authorization on a database query mechanism.
- An insufficient enforcement of database query type restrictions.
- The missing server side check on file type/extension when uploading and modifying scripts
- The directory traversal in SCRIPT_NAME field when modifying existing scripts

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.813213
Version used: `2021-09-23T03:58:52Z`

References
`cve: CVE-2018-5337`
`cve: CVE-2018-5338`
`cve: CVE-2018-5339`
`cve: CVE-2018-5341`
`url: https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vuln`
`↪erabilities-in-manageengine-desktop-central`

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 8.0.293 Arbitrary File Upload Vulnerability

Summary
ManageEngine Desktop Central is prone to an arbitrary file upload vulnerability.

Vulnerability Detection Result
`It was possible to upload the file "/openvasvt666997251.jsp". Please delete this`
`↪ file.`
`Vulnerable URL: http://king-arthur:8020/agentLogUploader?computerName=DesktopCen`
`↪tral&domainName=webapps&customerId=1&filename=openvasvt666997251.jsp`

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

Solution:
Solution type: VendorFix
Update to version 8.0.293 or later.

Affected Software/OS
ManageEngine Desktop Central prior to version 8.0.293.

Vulnerability Insight
The flaw in the AgentLogUploadServlet. This servlet takes input from HTTP POST and constructs an output file on the server without performing any sanitisation or even checking if the caller is authenticated.

Vulnerability Detection Method
Sends a crafted HTTP POST request and checks the response.
Details: `ManageEngine Desktop Central < 8.0.293 Arbitrary File Upload Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.803777
Version used: `2021-10-15T09:03:25Z`

References
`cve: CVE-2013-7390`
`cve: CVE-2014-5007`
`url: http://www.exploit-db.com/exploits/29674`
`url: http://security-assessment.com/files/documents/advisory/DesktopCentral%20Ar`
`↪bitrary%20File%20Upload.pdf`

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerability

Summary
ManageEngine Desktop Central 9 suffers from a vulnerability that allows a remote attacker to upload a malicious file, and execute it under the context of SYSTEM.

Vulnerability Detection Result
`It was possible to upload the file 'http://king-arthur:8020/jspf/OpenVASVT_CVE-2`
`↪015-8249_test.jsp'. Please delete this file.`

Impact
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

Solution:
Solution type: VendorFix
Update to version 9.0.142 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
ManageEngine Desktop Central prior to version 9.0.142.

Vulnerability Detection Method
Try to upload a jsp file.
Details: `ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerabi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.140041
Version used: `2021-10-12T12:01:25Z`

References
`cve: CVE-2015-8249`

High (CVSS: 7.5)
NVT: '/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Vulnerable URL: http://king-arthur:8020/.//WEB-INF/web.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
```

... continues on next page ...

... continued from previous page ...

```
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and/or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
The following vendor fixes are known:
- Update to Payara Platform Enterprise 5.31.0, Payara Platform Community 5.2021.7 or later.
For other products please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- Payara Platform Enterprise / Community
Other products might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.

... continues on next page ...

... continued from previous page ...

However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/.//WEB-INF/web.xml
http://example.com/.//web-inf/web.xml
(note the './/' before 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117707
Version used: `2023-03-06T10:19:58Z`

References
`cve: CVE-2021-41381`
`url: https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-`
`↪054.txt`
`url: http://packetstormsecurity.com/files/164365/Payara-Micro-Community-5.2021.6`
`↪-Directory-Traversal.html`

[return to 192.168.121.132]

2.1.8 High 3050/tcp

High (CVSS: 9.0)
NVT: Firebird Default Credentials (Firebird Protocol)

Summary
It is possible to connect to the remote database service using default credentials.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker may use this flaw to execute commands against the remote host, as well as read your database content.

Solution:
Solution type: Mitigation
Change the default password by using the gsec management tool.

Vulnerability Insight
The remote Firebird Server uses default credentials (SYSDBA/masterkey).

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details: Firebird Default Credentials (Firebird Protocol)
OID:1.3.6.1.4.1.25623.1.0.100792
Version used: 2023-07-28T16:09:07Z

References
url: http://www.firebirdsql.org/manual/qsg2-config.html#qsg2-config-security

[return to 192.168.121.132]

2.1.9 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result
```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.121.132[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:192.168.121.132[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.121.132[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.121.132[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.121.132[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:192.168.121.132[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.121.132[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.121.132[49154]
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:192.168.121.132[49154]
      Annotation: XactSrv service
      UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
      Endpoint: ncacn_ip_tcp:192.168.121.132[49154]
      Annotation: IKE/Authip API
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.121.132[49154]
      Annotation: Impl friendly name
Port: 49160/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.121.132[49160]
Port: 49162/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.121.132[49162]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Port: 49165/tcp
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.121.132[49165]
      Annotation: IPSec Policy agent endpoint
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:192.168.121.132[49165]
      Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[return to 192.168.121.132]

2.1.10 Medium 3389/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2021-12-01T13:10:37Z

References
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

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
```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
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: `2021-07-19T08:11:48Z`

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
```

... continues on next page ...

... continued from previous page ...

```
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
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
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=king-arthur
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

References
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[return to 192.168.121.132]

2.1.11 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Microsoft IIS Default Welcome Page Information Disclosure Vulnerability

Product detection result
`cpe:/a:microsoft:internet_information_services:7.5`
`Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900710)`

Summary
Microsoft IIS Webserver is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to obtain sensitive information that could aid in further attacks.

Solution:
Solution type: Mitigation
Disable the default pages within the server configuration.

Affected Software/OS
Microsoft Internet Information Services.

Vulnerability Insight
The flaw is due to misconfiguration of IIS Server, which allows to access default pages when the server is not used.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method
Details: `Microsoft IIS Default Welcome Page Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.802806
Version used: `2022-02-15T13:40:32Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:7.5`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

[return to 192.168.121.132]

2.1.12 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result

```
It was possible to login to the remote FTP service with the following anonymous
↪account(s):
anonymous:anonymous@example.com
Here are the contents of the remote FTP directory listing:
Account "anonymous":
drwxr-xr-x 1 ftp ftp              0 Jul 16  2020 aspnet_client
-rw-r--r-- 1 ftp ftp            689 Jul 16  2020 iisstart.htm
-rw-r--r-- 1 ftp ftp         184946 Jul 16  2020 welcome.png
```

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files.

Solution:
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method
Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0497`

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt
Anonymous sessions:     331 Password required for anonymous
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

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

[return to 192.168.121.132]

2.1.13 Medium 8443/tcp

Medium (CVSS: 5.4)
NVT: SSL/TLS: Report 'Anonymous' Cipher Suites

Summary
This routine reports all 'Anonymous' SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
`'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DH_anon_WITH_AES_128_CBC_SHA`

Impact
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed 'Anonymous' cipher suites anymore.
Please see the references for more resources supporting you in this task.

Vulnerability Insight
Services supporting 'Anonymous' cipher suites could allow a client to negotiate an SSL/TLS connection to the host without any authentication of the remote endpoint.

Vulnerability Detection Method
Details: `SSL/TLS: Report 'Anonymous' Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.108147
Version used: `2022-04-13T11:57:07Z`

References
`cve: CVE-2007-1858`
`cve: CVE-2014-0351`
`url: https://bettercrypto.org/`
`url: http://www.securityfocus.com/bid/28482`
`url: http://www.securityfocus.com/bid/69754`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`cert-bund: CB-K14/0058`
`dfn-cert: DFN-CERT-2014-0049`
`dfn-cert: DFN-CERT-2012-0442`

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
```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
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: `2021-07-19T08:11:48Z`

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
```

... continues on next page ...

... continued from previous page ...

```
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
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
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
`Server Temporary Key Size: 768 bits`

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 192.168.121.132]

2.1.14 Medium 8022/tcp

Medium (CVSS: 6.1)
NVT: ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities

Summary
ManageEngine Desktop Central is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result
```
Installed version: 9.1.051
Fixed version:     9.2.026
Installation
path / port:       /
```

Impact
Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

Solution:
Solution type: VendorFix
Update to version 9.2.026 or later.

Affected Software/OS
ManageEngine Desktop Central version 9.1.099 and prior.

Vulnerability Insight
The flaw allows to inject client-side script into Desktop Centrals web page.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.812576
Version used: `2022-04-13T07:21:45Z`

References
```
cve: CVE-2018-8722
url: https://www.manageengine.com/products/desktop-central/cross-site-scripting-
↪vulnerability.html
url: http://www.securityfocus.com/bid/103426
```

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

. . . continues on next page . . .

... continued from previous page ...

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
`The following input fields where identified (URL:input name):`
`http://king-arthur:8022/configurations.do:j_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: `2023-07-20T05:05:17Z`

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: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability

Summary
ManageEngine Desktop Central is prone to a reflected cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 9.1.051
Fixed version:     9.2.026
Installation
path / port:       /
```

Impact
Successful exploitation will allow attacker to cause cross site scripting and steal the cookie of other active sessions.

Solution:
Solution type: VendorFix
Update to version 9.2.026 or later.

Affected Software/OS
ManageEngine Desktop Central version 9.1.099 and prior.

Vulnerability Insight
The flaw exists as input passed via 'To' parameter of 'Specify Delivery Format' is not validated properly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.807741
Version used: `2021-09-23T03:58:52Z`

References
`url: https://packetstormsecurity.com/files/136463`

[return to 192.168.121.132]

2.1.15 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
```

... continues on next page ...

... continued from previous page ...

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.

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: `2022-12-08T10:12:32Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142.html`
`url: https://www.rfc-editor.org/rfc/rfc9142.html#name-summary-guidance-for-imple`
`↪m`
`url: https://datatracker.ietf.org/doc/html/rfc6194`

[return to 192.168.121.132]

2.1.16 Medium 8383/tcp

Medium (CVSS: 6.1)
NVT: ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities

Summary
ManageEngine Desktop Central is prone to multiple cross-site scripting (XSS) vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Installed version: 9.1.051
Fixed version:     9.2.026
Installation
path / port:       /
```

Impact

Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

Solution:

Solution type: VendorFix

Update to version 9.2.026 or later.

Affected Software/OS

ManageEngine Desktop Central version 9.1.099 and prior.

Vulnerability Insight

The flaw allows to inject client-side script into Desktop Centrals web page.

Vulnerability Detection Method

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

Details: `ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.812576

Version used: `2022-04-13T07:21:45Z`

References

```
cve: CVE-2018-8722
url: https://www.manageengine.com/products/desktop-central/cross-site-scripting-
↪vulnerability.html
url: http://www.securityfocus.com/bid/103426
```

Medium (CVSS: 5.3)

NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

Summary

The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Vulnerability Detection Result

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00F59CEF71E6DB72A5:1.2.840.113549.1.9.1=#737570706F7274406465736B746F70
```

... continues on next page ...

... continued from previous page ...

↪63656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L
↪=Pleasanton,ST=CA,C=US (Server certificate)

Impact
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

References
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: '/WEB-INf./' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result
Vulnerable URL: https://king-arthur:8383/WEB-INf./web.xml
Response (truncated):

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
```

... continues on next page ...

... continued from previous page ...

```
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
Please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- A misconfigured reverse proxy.

... continues on next page ...

... continued from previous page ...

Other products might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/META-INf./web.xml
(note the 'f.' in 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INf./' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117225
Version used: `2023-03-06T10:19:58Z`

References
`url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60667`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2020-09-05 12:24:44.
Certificate details:
fingerprint (SHA-1)             | 701E2E6DF8854C4F0B298DFF03A2C6F0BAC7D315
fingerprint (SHA-256)           | C1DF756862FA17582C31E8F8EBDA084D1A1341815B716E
↪B135AD83CD7B01A5A5
issued by                       | 1.2.840.113549.1.9.1=#737570706F7274406465736B
↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora
↪tion,L=Pleasanton,ST=CA,C=US
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00F59CEF71E6DB72A5
signature algorithm             | sha1WithRSAEncryption
subject                         | 1.2.840.113549.1.9.1=#737570706F7274406465736B
↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora
↪tion,L=Pleasanton,ST=CA,C=US
subject alternative names (SAN) | None
valid from                      | 2010-09-08 12:24:44 UTC
```

... continues on next page ...

... continued from previous page ...

valid until	2020-09-05 12:24:44 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2021-11-22T15:32:39Z

Medium (CVSS: 5.0)
NVT: '/WEB-INF../' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Vulnerable URL: https://king-arthur:8383/WEB-INF../web.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
```

... continues on next page ...

... continued from previous page ...

```
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
               <param-name>PARAMETER-ENCODING</param-name>
               <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
Please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- Caucho Resin version 2.1.12 on Apache HTTP server version 1.3.29
Other products and versions might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:

... continues on next page ...

... continued from previous page ...

http://example.com/WEB-INF../web.xml
http://example.com/web-inf../web.xml
(note the double dot ('..') after 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INF../' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117221
Version used: `2023-06-16T05:06:18Z`

References
`cve: CVE-2004-0281`
`url: http://marc.info/?l=bugtraq&m=107635084830547&w=2`
`url: http://www.securityfocus.com/bid/9617`

Medium (CVSS: 4.3)
NVT: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability

Summary
ManageEngine Desktop Central is prone to a reflected cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 9.1.051
Fixed version:     9.2.026
Installation
path / port:       /
```

Impact
Successful exploitation will allow attacker to cause cross site scripting and steal the cookie of other active sessions.

Solution:
Solution type: VendorFix
Update to version 9.2.026 or later.

Affected Software/OS
ManageEngine Desktop Central version 9.1.099 and prior.

Vulnerability Insight
The flaw exists as input passed via 'To' parameter of 'Specify Delivery Format' is not validated properly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.807741
Version used: 2021-09-23T03:58:52Z

References
url: https://packetstormsecurity.com/files/136463

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 ↪ 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: 2021-07-19T08:11:48Z

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126

... continues on next page ...

... continued from previous page ...

```
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
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#737570706F7274406465736B746F7063656E
↪7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleas
↪anton,ST=CA,C=US
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)

... continues on next page ...

... continued from previous page ...

- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

References
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-`
`↪sha-1-based-signature-algorithms/`

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
`Server Temporary Key Size: 1024 bits`

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: 2023-07-21T05:05:22Z

References
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

[return to 192.168.121.132]

2.1.17 Medium 8020/tcp

Medium (CVSS: 6.1)
NVT: ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities

Summary
ManageEngine Desktop Central is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result
Installed version: 9.1.051
Fixed version: 9.2.026
Installation
path / port: /

Impact
Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

Solution:
Solution type: VendorFix
Update to version 9.2.026 or later.

Affected Software/OS
ManageEngine Desktop Central version 9.1.099 and prior.

Vulnerability Insight
The flaw allows to inject client-side script into Desktop Centrals web page.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.812576
Version used: 2022-04-13T07:21:45Z

References
cve: CVE-2018-8722
url: https://www.manageengine.com/products/desktop-central/cross-site-scripting-vulnerability.html
url: http://www.securityfocus.com/bid/103426

Medium (CVSS: 5.0)
NVT: '/WEB-INF../' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result
Vulnerable URL: http://king-arthur:8020/WEB-INF../web.xml
Response (truncated):

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
```

... continues on next page ...

... continued from previous page ...

```
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
Please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- Caucho Resin version 2.1.12 on Apache HTTP server version 1.3.29
Other products and versions might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/WEB-INF../web.xml
http://example.com/web-inf../web.xml
(note the double dot ('..') after 'WEB-INF').

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Sends a crafted HTTP GET request and checks the response.
Details: '/WEB-INF../' Information Disclosure Vulnerability (HTTP)
OID:1.3.6.1.4.1.25623.1.0.117221
Version used: 2023-06-16T05:06:18Z

References
cve: CVE-2004-0281
url: http://marc.info/?l=bugtraq&m=107635084830547&w=2
url: http://www.securityfocus.com/bid/9617

Medium (CVSS: 5.0)
NVT: '/WEB-INf./' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result
Vulnerable URL: http://king-arthur:8020/WEB-INf./web.xml
Response (truncated):

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
```

... continues on next page ...

... continued from previous page ...

```
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
Please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- A misconfigured reverse proxy.
Other products might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/META-INf./web.xml
(note the 'f.' in 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INf./' Information Disclosure Vulnerability (HTTP)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.117225
Version used: 2023-03-06T10:19:58Z

References
url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60667

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
The following input fields where identified (URL:input name):
http://king-arthur:8020/configurations.do:j_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: 2023-07-20T05:05:17Z

References
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management

... continues on next page ...

... continued from previous page ...

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: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability

Summary
ManageEngine Desktop Central is prone to a reflected cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 9.1.051
Fixed version: 9.2.026
Installation
path / port: /

Impact
Successful exploitation will allow attacker to cause cross site scripting and steal the cookie of other active sessions.

Solution:
Solution type: VendorFix
Update to version 9.2.026 or later.

Affected Software/OS
ManageEngine Desktop Central version 9.1.099 and prior.

Vulnerability Insight
The flaw exists as input passed via 'To' parameter of 'Specify Delivery Format' is not validated properly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.807741
Version used: 2021-09-23T03:58:52Z

References
url: https://packetstormsecurity.com/files/136463

[return to 192.168.121.132]

2.1.18 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: 132558
Packet 2: 132678
```

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: `2023-05-11T09:09:33Z`

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
```

[return to 192.168.121.132]

2.1.19 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
`The following response / ICMP packet has been received:`
`- ICMP Type: 14`
`- ICMP Code: 0`

Impact
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`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.121.132]

This file was automatically generated.