Scan Report

October 18, 2019

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “TEST TASK 1”. The scan started at Thu Oct 17 11:57:12 2019 UTC and ended at Thu Oct 17 12:31:21 2019 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
[redacted]	9	10	0	37	0
[redacted]	0	4	1	32	0
[redacted]	26	52	5	78	0
Total: 3	35	66	6	147	0

Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
This report might not show details of all issues that were found.
Only results with a minimum QoD of 70 are shown.

This report contains all 254 results selected by the filtering described above. Before filtering there were 259 results.

2 Results per Host

2.1 [redacted]

Host scan start Thu Oct 17 11:57:28 2019 UTC
Host scan end Thu Oct 17 12:31:20 2019 UTC

Service (Port)	Threat Level
1433/tcp	High
80/tcp	High
general/tcp	High
3389/tcp	High
100/tcp	High
88/tcp	High
80/tcp	Medium
100/tcp	Medium
88/tcp	Medium
135/tcp	Medium
1433/tcp	Log
80/tcp	Log
general/CPE-T	Log
general/tcp	Log
139/tcp	Log
1162/tcp	Log
2383/tcp	Log

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
445/tcp	Log
3389/tcp	Log
100/tcp	Log
88/tcp	Log
135/tcp	Log
1025/tcp	Log
general/icmp	Log
2222/tcp	Log

2.1.1 High 1433/tcp

High (CVSS: 10.0)
NVT: Microsoft SQL Server End Of Life Detection

Product detection result
cpe:/a:microsoft:sql_server:10.0.1600.0
Detected by Microsoft SQL TCP/IP listener is running (OID: 1.3.6.1.4.1.25623.1.0 ,→.10144)

Summary
The Microsoft SQL Server version on the remote host has reached the end ofl ife and should not be used anymore.

Vulnerability Detection Result
The "Microsoft SQL Server 2008" version on the remote host has reached the end o ,→fl ife.
CPE: cpe:/a:microsoft:sql_server:10.0.1600.0
Installed version: 10.0.1600.0
EOL version: 10.0
EOL date: 2019-07-09

Impact
An end ofl ife version of Microsoft SQL Server is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution
Solution type: VendorFix
Update the Microsoft SQL Server version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Microsoft SQL Server End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.108188

... continues on next page ...

. . . continued from previous page . . .

Version used2018-10-12T09:42:02Z

Product Detection Result
Product: cpe:/a:microsoft:sql_server:10.0.1600.0
Method: Microsoft SQL TCP/IP listener is running
OID: 1.3.6.1.4.1.25623.1.0.10144)

References
Other:
URL:https://support.microsoft.com/en-us/lifecycle/search?sort=PN&alpha=sql%20s
,→erver&Filter=FilterNO
URL:https://en.wikipedia.org/wiki/History_of_Microsoft_SQL_Server#Release_sum
,→mary

2.1.2 High 80/tcp

High (CVSS: 10.0)
NVT: Microsoft IIS Web Server End Of Life Detection

Product detection result
cpe:/a:microsoft:iis:6.0
Detected by Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.
,→0.900710)

Summary
The Microsoft IIS Web Server version on the remote host has reached the end ofl ife and should not be used anymore.

Vulnerability Detection Result
The "Microsoft IIS Web Server" version on the remote host has reached the end of
,→ life.
CPE: cpe:/a:microsoft:iis:6.0
Installed version: 6.0
EOL version: 6.0
EOL date: 2015-07-14

Impact
An end ofl ife version of Microsoft IIS Web Server is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

. . . continues on next page . . .

... continued from previous page ...

Solution type: VendorFix
The Microsoft IIS Web Server version is tightly coupled to the operation system on the remote host. Updating the operation system to a supported version is required.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Microsoft IIS Web Server End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.108114
Version used2018-10-12T11:28:04Z

Product Detection Result
Product: cpe:/a:microsoft:iis:6.0
Method: Microsoft IIS Webserver Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
Other:
URL:https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Int
,→ernet%20Information%20Services

High (CVSS: 7.6)
NVT: Microsoft IIS WebDAV Remote Authentication Bypass Vulnerability

Product detection result
cpe:/a:microsoft:iis:6.0
Detected by Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.
,→0.900710)

Summary
The host is running Microsoft IIS Webserver with WebDAV Module and is prone to remote authentication bypass vulnerability.

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

Impact
Successful exploitation will let the attacker craft malicious UNICODE characters and send it over the context of IIS Webserver where WebDAV is enabled. As a result due to lack of security implementation check it will let the user fetch password protected directories without any valid authentications.

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

... continues on next page ...