Scan Report

18 Oct 2019

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the time zone "Coordinated Universal Time", which is abbreviated "UTC".

The task was "TEST TASK 1". The scan started at Thu, 17 Oct 2019 11:57:12 UTC and ended at Thu, 17 Oct 2019 12:31:21 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.

Results Overview

Host	Severity High	Severity Medium	Severity Low	Severity Log	False Positive
[redacted]	9	10	0	37	0
[redacted]	0	4	1	32	0
[redacted]	26	52	5	78	0
Total	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.Notes are included in the report.
- 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 Detection Threshold of 70 are shown.
- This report contains all 107 results selected by the Filtering described above.

Results Per Host

Host: [redacted]

Service (Port)	Threat Level
88/tcp	High
80/tcp	High
100/tcp	High
1433/tcp	High
3389/tcp	High
general/tcp	High
100/tcp	Medium
88/tcp	Medium
135/tcp	Medium
80/tcp	Medium

Service (Port): 88/tcp **FAIL**
Severity High (CVSS: 10.0)
Scan Plugin: Microsoft IIS Web Server End Of Life Detection

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

Summary:

The Microsoft IIS Web Server version on the remote host has reached the end of life 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

Service (Port): 88/tcp **FAIL**
Severity High (CVSS: 10.0)
Scan Plugin: Microsoft IIS Web Server End Of Life Detection

Impact:

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

Solution

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

References:

URL:https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Internet%20Information%20Services

Service (Port): 80/tcp **FAIL**
Severity High (CVSS: 10.0)
Scan Plugin: Microsoft IIS Web Server End Of Life Detection

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

Summary:

The Microsoft IIS Web Server version on the remote host has reached the end of life 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 of life version of Microsoft IIS Web Server is not receiving any security updates from the vendor. Unfixed security... might be leveraged by an attacker to compromise the security of this host.

Solution

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

References:

URL:https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Internet%20Information%20Services

Service (Port): 100/tcp **FAIL**
Severity High (CVSS: 10.0)
Scan Plugin: Microsoft IIS Web Server End Of Life Detection

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

Summary:

The Microsoft IIS Web Server version on the remote host has reached the end of life 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 of life version of Microsoft IIS Web Server is not receiving any security updates from the vendor. Unfixed security... might be leveraged by an attacker to compromise the security of this host.

Solution

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

References:

URL:https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Internet%20Information%20Services

Service (Port): 88/tcp **FAIL**
Severity High (CVSS: 7.6)
Scan Plugin: Microsoft IIS WebDAV Remote Authentication Bypass Vulnerability

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

Summary:

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