

Scan Report

April 26, 2023

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 “Windows”. The scan started at Wed Apr 26 03:02:10 2023 UTC and ended at Wed Apr 26 03:07:09 2023 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	2
2	Results per Host	2
2.1	192.168.10.142	2
2.1.1	High 80/tcp	2
2.1.2	Low general/icmp	4
2.1.3	Low general/tcp	4

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.10.142	1	0	2	0	0
Total: 1	1	0	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 3 results selected by the filtering described above. Before filtering there were 14 results.

2 Results per Host

2.1 192.168.10.142

Host scan start Wed Apr 26 03:02:38 2023 UTC

Host scan end Wed Apr 26 03:07:02 2023 UTC

Service (Port)	Threat Level
80/tcp	High
general/icmp	Low
general/tcp	Low

2.1.1 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)

... continues on next page ...

...continued from previous page ...
Summary This host is missing an important security update according to Microsoft Bulletin MS15-034.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Solution: Solution type: VendorFix The vendor has released updates. Please see the references for more information.
Affected Software/OS - Microsoft Windows 8 x32/x64 - Microsoft Windows 8.1 x32/x64 - Microsoft Windows Server 2012 - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior - Microsoft Windows 7 x32/x64 Service Pack 1 and prior
Vulnerability Insight Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.
Vulnerability Detection Method 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: 2022-08-09T10:11:17Z
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
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545

[\[return to 192.168.10.142 \]](#)

2.1.2 Low general/icmp

Low (CVSS: 2.1) NVT: ICMP Timestamp Reply Information Disclosure
<p>Summary The remote host responded to an ICMP timestamp request.</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>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)</p>
<p>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. This information could theoretically be used to exploit weak time-based random number generators in other services.</p>
<p>Vulnerability Detection Method Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2022-11-18T10:11:40Z</p>
<p>References cve: CVE-1999-0524 url: http://www.ietf.org/rfc/rfc0792.txt cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658</p>

[\[return to 192.168.10.142 \]](#)

2.1.3 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
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: 187236 Packet 2: 187341
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 OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2020-08-24T08:40:10Z
References url: http://www.ietf.org/rfc/rfc1323.txt url: http://www.ietf.org/rfc/rfc7323.txt url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

[[return to 192.168.10.142](#)]

This file was automatically generated.