Scan Report

February 22, 2025

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 "Immediate scan of IP 6.87.151.210". The scan started at Sat Feb 22 07:57:05 2025 UTC and ended at Sat Feb 22 08:02:48 2025 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
6.87.151.210	3	3	0	0	0
Total: 1	3	3	0	0	0

Vendor security updates are not trusted.
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.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
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 6 results selected by the filtering described above. Before filtering there were 25 results.

2 Results per Host

2.1 6.87.151.210

Host scan start	Sat Feb 22 07:57:31 2025 UTC
Host scan end	Sat Feb 22 08:02:48 2025 UTC

Service (Port)	Threat Level
445/tcp	High
6002/tcp	High
general/tcp	High
6002/tcp	Medium

2.1.1 High 445/tcp

High (CVSS: 9.3)
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.

. . . continues on next page . . .

... continued from previous page ...

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 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition 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: `2019-05-03T10:54:50+0000`

References
```
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
  URL:https://support.microsoft.com/en-in/kb/4013078
   URL:https://technet.microsoft.com/library/security/MS17-010
   URL:https://github.com/rapid7/metasploit-framework/pull/8167/files
```

[return to 6.87.151.210]

2.1.2 High 6002/tcp

High (CVSS: 7.8)
NVT: Generic HTTP Directory Traversal

Summary
Generic check for HTTP directory traversal vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The following traversal URL(s) where found:
Vulnerable url: http://6.87.151.210:6002/../../../../../../windows/win.ini
Request:
GET /../../../../../../windows/win.ini HTTP/1.0

Response:
HTTP/1.0 200 OK
Date: Sat, 22 Feb 2025 08:01:51 GMT
Server: SentinelProtectionServer/7.3
MIME-Version: 1.1
Content-Type: application/octet-stream
Keep-Alive:0
Content-Length: 477


; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
[MCI Extensions.BAK]
aif=MPEGVideo
aifc=MPEGVideo
aiff=MPEGVideo
asf=MPEGVideo
asx=MPEGVideo
au=MPEGVideo
m1v=MPEGVideo
m3u=MPEGVideo
mp2=MPEGVideo
mp2v=MPEGVideo
mp3=MPEGVideo
mpa=MPEGVideo
mpe=MPEGVideo
mpeg=MPEGVideo
mpg=MPEGVideo
mpv2=MPEGVideo
snd=MPEGVideo
wax=MPEGVideo
wm=MPEGVideo
wma=MPEGVideo
wmv=MPEGVideo
wmx=MPEGVideo
```

... continues on next page ...

... continued from previous page ...

```
wpl=MPEGVideo
wvx=MPEGVideo
Vulnerable url: http://6.87.151.210:6002/../../../../../../boot.ini
Request:
GET /../../../../../../boot.ini HTTP/1.0

Response:
HTTP/1.0 200 OK
Date: Sat, 22 Feb 2025 08:01:51 GMT
Server: SentinelProtectionServer/7.3
MIME-Version: 1.1
Content-Type: application/octet-stream
Keep-Alive:0
Content-Length: 211


[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
↪/noexecute=optin /fastdetect
Vulnerable url: http://6.87.151.210:6002/..\..\..\..\..\..\windows/win.ini
Request:
GET /..\..\..\..\..\..\windows/win.ini HTTP/1.0

Response:
HTTP/1.0 200 OK
Date: Sat, 22 Feb 2025 08:01:51 GMT
Server: SentinelProtectionServer/7.3
MIME-Version: 1.1
Content-Type: application/octet-stream
Keep-Alive:0
Content-Length: 477


; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
[MCI Extensions.BAK]
aif=MPEGVideo
aifc=MPEGVideo
aiff=MPEGVideo
```

... continues on next page ...

... continued from previous page ...

```
asf=MPEGVideo
asx=MPEGVideo
au=MPEGVideo
m1v=MPEGVideo
m3u=MPEGVideo
mp2=MPEGVideo
mp2v=MPEGVideo
mp3=MPEGVideo
mpa=MPEGVideo
mpe=MPEGVideo
mpeg=MPEGVideo
mpg=MPEGVideo
mpv2=MPEGVideo
snd=MPEGVideo
wax=MPEGVideo
wm=MPEGVideo
wma=MPEGVideo
wmv=MPEGVideo
wmx=MPEGVideo
wpl=MPEGVideo
wvx=MPEGVideo
Vulnerable url: http://6.87.151.210:6002/..\..\..\..\..\..\boot.ini
Request:
GET /..\..\..\..\..\..\boot.ini HTTP/1.0

Response:
HTTP/1.0 200 OK
Date: Sat, 22 Feb 2025 08:01:51 GMT
Server: SentinelProtectionServer/7.3
MIME-Version: 1.1
Content-Type: application/octet-stream
Keep-Alive:0
Content-Length: 211


[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
↪/noexecute=optin /fastdetect
```

Solution
Solution type: Mitigation
Contact the vendor for a solution.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Sends crafted HTTP requests and checks the response.
Details: Generic HTTP Directory Traversal
OID:1.3.6.1.4.1.25623.1.0.106756
Version used: $Revision: 12019 $

References
Other:
URL:https://www.owasp.org/index.php/Path_Traversal

[return to 6.87.151.210]

2.1.3 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result
cpe:/o:microsoft:windows_xp
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

Summary
OS End Of Life Detection
The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The "Windows XP" Operating System on the remote host has reached the end of life
↪.
CPE: cpe:/o:microsoft:windows_xp
EOL date: 2014-04-08
EOL info: https://support.microsoft.com/en-us/lifecycle/search?sort=PN&
↪alpha=Microsoft%20Windows%20XP&Filter=FilterNO

Solution
Solution type: Mitigation

Vulnerability Detection Method
Details: OS End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 8927 $

Product Detection Result
Product: cpe:/o:microsoft:windows_xp
Method: OS Detection Consolidation and Reporting

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 6.87.151.210]

2.1.4 Medium 6002/tcp

Medium (CVSS: 5.0)
NVT: Cogent DataHub Multiple Vulnerabilities

Summary
Cogent DataHub is prone to a directory-traversal vulnerability, an information-disclosure vulnerability and to multiple buffer-overflow and integer-overflow vulnerabilities.

Vulnerability Detection Result
`Vulnerable url: http://6.87.151.210:6002/..\\..\\..\\..\\..\\..\\..\\..\\..\\..\`
`↪\windows/win.ini`

Impact
Exploiting the issues may allow an attacker to obtain sensitive information that could aid in further attacks or may allow attackers to execute arbitrary code within the context of the privileged domain.

Solution
Solution type: VendorFix
Update to versions 6.4.20/7.1.2 or later

Affected Software/OS
Cogent DataHub 7.1.1.63 is vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Details: `Cogent DataHub Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.103253
Version used: `$Revision: 13543 $`

References
```
CVE: CVE-2011-3500, CVE-2011-3501
BID:49610, 49611
Other:
  URL:http://www.securityfocus.com/bid/49610
   URL:http://www.securityfocus.com/bid/49611
   URL:http://www.cogentdatahub.com/Products/Cogent_DataHub.html
   URL:http://aluigi.org/mytoolz/mydown.zip
```

Medium (CVSS: 5.0)
NVT: JRun directory traversal

Summary
This host is running the Allaire JRun web server. Versions 2.3.3, 3.0, and 3.1 are vulnerable to a directory traversal attack.

Vulnerability Detection Result
`Vulnerable url: http://6.87.151.210:6002/../../../../../../../../windows/win.ini`

Impact
This allows a potential intruder to view the contents of any file on the system.

Solution
Solution type: VendorFix
The vendor has addressed this issue in Macromedia Product Security Bulletin MPSB01-17. Please upgrade to the latest version of JRun.

Vulnerability Detection Method
Details: `JRun directory traversal`
OID:1.3.6.1.4.1.25623.1.0.10997
Version used: `$Revision: 13543 $`

References
`CVE: CVE-2001-1544`
`BID:3666`
`Other:`
`URL:http://www.allaire.com/`

Medium (CVSS: 4.3)
NVT: Calibre Cross Site Scripting and Directory Traversal Vulnerabilities

Summary
Calibre is prone to a cross-site scripting vulnerability and a directory- traversal vulnerability because it fails to sufficiently sanitize user- supplied input.
Exploiting these issues will allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, and to view arbitrary local files and directories within the context of the webserver. This may let the attacker steal cookie-based authentication credentials and other harvested information may aid in launching further attacks.
Calibre 0.7.34 is vulnerable. Other versions may also be affected.

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

Solution
Solution type: WillNotFix

. . . continues on next page . . .

... continued from previous page ...

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Vulnerability Detection Method
Details: Calibre Cross Site Scripting and Directory Traversal Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.103011
Version used: $Revision: 12018 $

References
BID:45532
Other:
URL:https://www.securityfocus.com/bid/45532
URL:http://www.waraxe.us/advisory-77.html
URL:http://calibre-ebook.com/

[return to 6.87.151.210]