Scan Report

January 27, 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 "Immediate scan of IP 172.16.1.5". The scan started at Mon Jan 16 14:40:20 2023 UTC and ended at Mon Jan 16 14:50:49 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

Host	High	Medium	Low	Log	False Positive
172.16.1.5	1	1	2	0	0
Total: 1	1	1	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 4 results selected by the filtering described above. Before filtering there were 83 results.

2 Results per Host

2.1 172.16.1.5

Host scan start	Mon Jan 16 14:41:12 2023 UTC
Host scan end	Mon Jan 16 14:50:44 2023 UTC

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

2.1.1 High 21/tcp

High (CVSS: 10.0)
NVT: ProFTPD Backdoor Unauthorized Access Vulnerability

Product detection result

```
cpe:/a:proftpd:proftpd:1.3.3:c
Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.
↪0.900815)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

ProFTPD is prone to an unauthorized-access vulnerability due to a backdoor in certain versions of the application.

Vulnerability Detection Result

```
It was possible to execute the command 'id' on the remote host,
which produces the following output:
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
```

Impact

Exploiting this issue allows remote attackers to execute arbitrary system commands with superuser privileges.

Solution:

Solution type: VendorFix

The vendor released an advisory to address the issue. Please see the references for more information.

Affected Software/OS

The issue affects the ProFTPD 1.3.3c package downloaded between November 28 and December 2, 2010.

The MD5 sums of the unaffected ProFTPD 1.3.3c source packages are as follows:

8571bd78874b557e98480ed48e2df1d2 proftpd-1.3.3c.tar.bz2 4f2c554d6273b8145095837913ba9e5d proftpd-1.3.3c.tar.gz

Files with MD5 sums other than those listed above should be considered affected.

Vulnerability Detection Method

Details: `ProFTPD Backdoor Unauthorized Access Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.100933

Version used: `2022-12-02T10:11:16Z`

Product Detection Result

Product: `cpe:/a:proftpd:proftpd:1.3.3:c`

Method: `ProFTPD Server Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.900815)

References

```
url: http://www.securityfocus.com/bid/45150
url: http://sourceforge.net/mailarchive/message.php?msg_name=alpine.DEB.2.00.101
↪2011542220.12930%40familiar.castaglia.org
```

[return to 172.16.1.5]

2.1.2 Medium 21/tcp

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):
Anonymous sessions:     331 Anonymous login ok, send your complete email address
↪ as your password
Non-anonymous sessions: 331 Password required for gbnvt
```

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: `2020-08-24T08:40:10Z`

[return to 172.16.1.5]

2.1.3 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
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:
Solution type: Mitigation
Various mitigations are possible:

. . . continues on next page . . .

. . . continued from previous page . . .

- 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. This information could theoretically be used to exploit weak time-based random number generators in other services.

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`

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

[return to 172.16.1.5]

2.1.4 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: 2764653299
Packet 2: 2764654395
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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/d
↪ownload/details.aspx?id=9152
```

[return to 172.16.1.5]