Scan Report

January 12, 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 192.168.1.102". The scan started at Thu Jan 12 16:49:11 2023 UTC and ended at Thu Jan 12 17:08:56 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
192.168.1.102	2	1	1	0	0
Total: 1	2	1	1	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 37 results.

2 Results per Host

2.1 192.168.1.102

Host scan start	Thu Jan 12 16:49:57 2023 UTC
Host scan end	Thu Jan 12 17:08:52 2023 UTC

Service (Port)	Threat Level
5000/tcp	High
135/tcp	Medium
general/icmp	Low

2.1.1 High 5000/tcp

High (CVSS: 7.6)
NVT: Python <= 3.11 Shell Command Injection Vulnerability - Windows

Product detection result
`cpe:/a:python:python:3.10.8`
`Detected by Python Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.112857)`

Summary

. . . continues on next page . . .

... continued from previous page ...

Python is prone to a shell command injection vulnerability in the mailcap module.

Vulnerability Detection Result

```
Installed version: 3.10.8
Fixed version:     None
Installation
path / port:       5000/tcp
```

Solution:

Solution type: NoneAvailable

No known solution is available as of 21th April, 2022. Information regarding this issue will be updated once solution details are available.

Affected Software/OS

Python versions 3.11 and prior.

Vulnerability Insight

In Python (aka CPython) the mailcap module does not add escape characters into commands discovered in the system mailcap file. This may allow attackers to inject shell commands into applications that call mailcap.findmatch with untrusted input (if they lack validation of user-provided filenames or arguments).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Python <= 3.11 Shell Command Injection Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.113932

Version used: `2022-11-15T10:10:43Z`

Product Detection Result

Product: `cpe:/a:python:python:3.10.8`

Method: `Python Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.112857)

References

```
cve: CVE-2015-20107
url: https://bugs.python.org/issue24778
url: https://github.com/python/cpython/issues/68966
dfn-cert: DFN-CERT-2022-2572
dfn-cert: DFN-CERT-2022-2264
dfn-cert: DFN-CERT-2022-2184
dfn-cert: DFN-CERT-2022-2020
dfn-cert: DFN-CERT-2022-1537
dfn-cert: DFN-CERT-2022-1307
```

High (CVSS: 7.5)
NVT: Python < 3.11 Buffer Overflow Vulnerability - Windows

Product detection result
cpe:/a:python:python:3.10.8
Detected by Python Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.112857)

Summary
Python is prone to a buffer overflow vulnerability in the _sha3 module.

Vulnerability Detection Result
Installed version: 3.10.8
Fixed version: See advisory
Installation
path / port: 5000/tcp

Solution:
Solution type: VendorFix
Update to version 3.11.0 or later. See the referenced vendor advisory for patched previous versions.

Affected Software/OS
Python prior to version 3.11.

Vulnerability Insight
The Keccak XKCP SHA-3 reference implementation has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Python < 3.11 Buffer Overflow Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.148943
Version used: 2022-11-23T10:13:09Z

Product Detection Result
Product: cpe:/a:python:python:3.10.8
Method: Python Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.112857)

References
cve: CVE-2022-37454
url: https://python-security.readthedocs.io/vuln/sha3-buffer-overflow.html
url: https://github.com/python/cpython/issues/98517
dfn-cert: DFN-CERT-2022-2715

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2535
dfn-cert: DFN-CERT-2022-2523
dfn-cert: DFN-CERT-2022-2420
dfn-cert: DFN-CERT-2022-2380
```

[return to 192.168.1.102]

2.1.2 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 10791/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[10791]
     Annotation: Remote Fw APIs
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.102[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49665]
Port: 49666/tcp
```

... continues on next page ...

... continued from previous page ...

```
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49667]
Port: 49668/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49668]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49668]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49668]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49668]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.102[49668]
Port: 49676/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.102[49676]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[return to 192.168.1.102]

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:
- 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 192.168.1.102]