Security Advisory 2025-003

Critical Vulnerabilities in Fortinet Products

2025-01-15 — v1.0

TLP:CLEAR

History:

- *15/01/2025 — v1.0 – Initial publication*

Summary

On January 14, Fortinet released and updated several security advisories addressing multiple vulnerabilities ranging from low to critical severity [1]. At least one critical vulnerability is known to be exploited in the wild.

It recommended updating as soon as possible, and if not possible, at least applying mitigations.

Technical Details

- The vulnerability **CVE-2024-55591**, with a CVSS score of 9.6, is an authentication bypass in `Node.js` websocket module in FortiOS and FortiProxy which allow a remote attacker to gain super-admin privileges via crafted requests to `Node.js` websocket module. This vulnerability affects the management interface. This vulnerability is exploited in the wild [2].
- The vulnerability **CVE-2023-37936**, with a CVSS score of 9.6, is a use of hard-coded cryptographic key vulnerability in FortiSwitch and allows a remote unauthenticated attacker in possession of the key to execute unauthorised code via crafted cryptographic requests [3].

Fortinet also addresses 13 other high severity vulnerabilities.

Affected Products

- The vulnerability **CVE-2024-55591** affects FortiOS versions 7.0.0 through 7.0.16, and FortiProxy 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12.
- The vulnerability **CVE-2023-37936** affects FortiSwitch versions:
  - 6.0.0 through 6.0.7;
  - 6.2.0 through 6.2.7;
  - 6.4.0 through 6.4.13;
  - 7.0.0 through 7.0.7;
  - 7.2.0 through 7.2.5;
  - 7.4.0.

Recommendations

It is recommended updating as soon as possible. Considering that the vulnerability **CVE-2024-55591** is exploited in the wild, it recommended to look for indicators of compromise (IoCs). When IoCs are found, it is recommended to trigger the Incident Response process.

Detection

Fortinet has provided possible IoCs to look for potential exploitation of the vulnerability **CVE-2024-55591**:

In the logs

- Following login activity log with random `scrip` and `dstip`:

```
type="event" subtype="system" level="information" vd="root" logdesc="Admin login successful"
  sn="1733486785" user="admin" ui="jsconsole" method="jsconsole" srcip=1.1.1.1 dstip=1.1.1.1
  action="login" status="success" reason="none" profile="super_admin" msg="Administrator admin
  logged in successfully from jsconsole"
```

- Following admin creation log with seemingly randomly generated user name and source IP:

```
type="event" subtype="system" level="information" vd="root" logdesc="Object attribute
  configured" user="admin" ui="jsconsole(127.0.0.1)" action="Add" cfgtid=1411317760
  cfgpath="system.admin" cfgobj="vOcep" cfgattr="password[*]accprofile[super_admin]vdom[root]"
  msg="Add system.admin vOcep"
```

The following IP addresses were mostly found used by attackers in the above logs:

- `1.1.1.1`
- `127.0.0.1`
- `2.2.2.2`
- `8.8.8.8`
- `8.8.4.4`

Please note that the above IP parameters are under attacker control and therefore can be any other IP address. Please note as well that sn and `cfgtid` are not relevant to the attack.

- Logging in the `sslvpn` with the above added local users to get a tunnel to the internal network. the Threat Action has been seen using the following IP addresses:
  - `45.55.158.47` [most used IP address]
  - `87.249.138.47`
  - `155.133.4.175`
  - `37.19.196.65`
  - `149.22.94.37`

In the device configuration

The operations performed by the Threat Actor (TA) in the cases we observed were part or all of the below:

- Creating an admin account on the device with random user name
- Creating a Local user account on the device with random user name

- Creating a user group or adding the above local user to an existing sslvpn user group
- Adding/changing other settings (firewall policy, firewall address, . . .)

Workarounds

As a workaround, Fortinet recommends to disable HTTP/HTTPS administrative interface or Limit IP addresses that can reach the administrative interface via local-in policies [2].

References

[1] https://www.fortiguard.com/psirt?filter=1&product=FortiOS-6K7K%2CFortiOS&product=FortiSwitch&product=FortiSwitchManager&product=FortiAP&product=FortiAP-U&product=FortiAP-W2&product=FortiAP-S&product=FortiAP-C&product=FortiManager&product=FortiAnalyzer&product=FortiAnalyzer-BigData&product=FortiManager+Cloud&product=FortiAnalyzer+Cloud&product=FortiSandbox&product=FortiExtender&version=&date=2025

[2] https://www.fortiguard.com/psirt/FG-IR-24-535

[3] https://www.fortiguard.com/psirt/FG-IR-23-260