Security Advisory 2022-070

FortiOS and FortiProxy Critical Vulnerability

October 14, 2022 — v1.1

TLP:CLEAR

History:

- *11/10/2022 — v1.0 – Initial publication*
- *14/10/2022 — v1.1 – Updates with the new available Proof-of-concept exploit code*

Summary

On 10th of October, 2022, Fortinet released a security advisory to warn about a critical vulnerability (CVSS v3 score: 9.6), tracked as CVE-2022-40684, impacting the FortiOS, FortiProxy and FortiSwitchManager [1]. The exploitation of this vulnerability allows an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

Fortinet is aware of at least one instance where this vulnerability was exploited and hence it is recommended to remediate this vulnerability with the utmost urgency.

Updates of 14/10/2022

A proof-of-concept (PoC) exploit and a technical root cause analysis for this vulnerability has been published by the Horizon3.ai security researchers [4].

Technical Details

The vulnerability is due to an authentication bypass via specially crafted HTTP or HTTPS requests on an alternate path or channel vulnerability (CWE-288) in FortiOS, FortiProxy and FortiSwitchManager. This may allow an unauthenticated attacker to perform operations on the administrative interface [1].

Affected Products

This vulnerability affects the following Fortinet products:

- FortiOS version 7.0.0 through 7.0.6 and from version 7.2.0 through 7.2.1
- FortiProxy version 7.0.0 through 7.0.6 and version 7.2.0
- FortiSwitchManager versions 7.0.0 and 7.2.0

Recommendations

Please upgrade to:

- FortiOS version 7.0.7 or 7.2.2 or above
- FortiProxy version 7.0.7 or 7.2.1 or above
- FortiSwitchManager version 7.2.1 or above

Exploitation Status

The PoC of exploitation is ready to be released [2, 3].

Fortinet recommends immediately validating your systems against the following indicator of compromise in the device's logs:

```
user="Local_Process_Access"
```

Workarounds

If the devices cannot be updated in a timely matter, there are workarounds that address this vulnerability by disabling HTTP/HTTPS administrative interface OR by limiting the IP addresses that can reach the administrative interface, until the upgrade can be performed. More details can be found in the Fortinet advisory [1].

References

[1] https://www.fortiguard.com/psirt/FG-IR-22-377

[2] https://www.bleepingcomputer.com/news/security/fortinet-says-critical-auth-bypass-bug-is-exploited-in-attacks/

[3] https://twitter.com/Horizon3Attack/status/1579285863108087810?s=20&t=2kQIYMv9xTAl4AVbX-ZI9g

[4] https://www.horizon3.ai/fortios-fortiproxy-and-fortiswitchmanager-authentication-bypass-technical-deep-dive-cve-2022-40684/