CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-036

High Severity Vulnerability in FortiManager and FortiAnalyzer

July 22, 2021 — v1.0

TLP:WHITE

History:

- *22/07/2021 — v1.0 – Initial publication*

Summary

On 19th of July 2021, Fortinet released information about a vulnerability (CVE-2021-32589) in FortiManager and FortiAnalyzer that could be exploited remotely by non-authenticated attackers to execute unauthorized / malicious code as `root` [1]. The severity of this vulnerability is **high**, with CVSSv3 Score 7.5 [2].

Technical Details

The flaw resides in `fgfmsd` daemon. If it is running and vulnerable, it can be exploited over the network. A use-after-free (CWE-416) vulnerability in the `fgfmsd` daemon may allow a remote, non-authenticated attacker to execute unauthorised code as root via sending a specifically crafted request to the FGFM port of the targeted device [3].

Products Affected

The following FortiManager versions are affected according to Fortinet [1]:

- FortiManager versions 5.6.10 and below.
- FortiManager versions 6.0.10 and below.
- FortiManager versions 6.2.7 and below.
- FortiManager versions 6.4.5 and below.
- FortiManager version 7.0.0.
- FortiManager versions 5.4.x.

The following FortiAnalyzer versions are affected according to Fortinet [1]:

- FortiAnalyzer versions 5.6.10 and below.
- FortiAnalyzer versions 6.0.10 and below.
- FortiAnalyzer versions 6.2.7 and below.
- FortiAnalyzer versions 6.4.5 and below.
- FortiAnalyzer version 7.0.0.

Recommendations

Please upgrade to the versions mentioned in [1].

CERT-EU recommends updating the vulnerable application as soon as possible.

Workarounds and Mitigations

Disable FortiManager features on the FortiAnalyzer unit using the command below:

```
config system global
set fmg-status disable <--- Disabled by default.
end
```

Fortinet mentions also the possibility of protection with FortiGate: Upgrade to IPS definitions version 18.100 or above, and make sure the action for signature FG-VD-50483 is set to block.

References

[1] https://www.fortiguard.com/psirt/FG-IR-21-067

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32589

[3] https://www.theregister.com/2021/07/20/fortinet_rce/