Security Advisory 2023-042

RCE vulnerability in Fortinet FortiNAC

June 26, 2023 — v1.0

TLP:CLEAR

History:

- *26/06/2023 — v1.0 – Initial publication*

Summary

On June 23, 2023, Fortinet released one advisory regarding a critical vulnerability in FortiNAC that may allow unauthenticated attackers to perform remote arbitrary code or command execution [1]. This vulnerability was identified as `CVE-2023-33299` with CVSS score of 9.6. FortiNAC is a network access control solution utilised by organisations to manage network access policies and compliance.

Due to the level of access and control on the network we recommend to update as soon as possible.

Technical Details

This vulnerability is the result of the deserialisation of untrusted data. An unauthenticated user can insert a modified serialised object into the system via specifically crafted requests to the tcp/1050 service, which leads to unauthenticated RCE.

Affected Products

- Version 9.4.0 through 9.4.2
- Version 9.2.0 through 9.2.7
- Version 9.1.0 through 9.1.9
- Version 7.2.0 through 7.2.1
- 8.8 all versions
- 8.7 all versions
- 8.6 all versions
- 8.5 all versions
- 8.3 all versions

Recommendations

Upgrade FortiNAC products to:

- Version 9.4.3 or above
- Version 9.2.8 or above
- Version 9.1.10 or above
- Version 7.2.2 or above

References

[1] https://www.fortiguard.com/psirt/FG-IR-23-074