Security Advisory 2023-022

Critical Authentication Vulnerability in Fortinet Product

April 17, 2023 — v1.0

TLP:CLEAR

History:

- *17/04/2023 — v1.0 – Initial publication*

Summary

On April 11, 2023, Fortinet released an advisory regarding one critical vulnerability in FortiPresence on-prem infrastructure server. This vulnerability is identified as **CVE-2022-41331** (CVSS score of 9.3) and it may allow remote un-authenticated attackers to access the Redis and MongoDB instances [1].

Moreover, Fortinet has also released security updates to address 9 High, and 10 Medium severity vulnerabilities in FortiPresence, FortiOS, FortiWeb, and other Fortinet products [1, 2].

Technical Details

The Critical severity vulnerability known as `CVE-2022-41331` exists due to missing authorisation checks to access Redis and MongoDB instances. A remote un-authenticated attacker can connect to the database instances via crafted authentication requests that may result in compromising the affected system [1, 2].

Affected Products

- FortiPresence 1.2 all versions [1];
- FortiPresence 1.1 all versions [1];
- FortiPresence 1.0 all versions [1].

Recommendations

It is recommended to upgrade FortiPresence instances to version 2.0.0 or above. In addition, CERT-EU encourages affected constituents to review the April 2023 Vulnerability Advisories of Fortinet and apply the relevant updates.

References

[1] https://www.fortiguard.com/psirt/FG-IR-22-355

[2] https://digital.nhs.uk/cyber-alerts/2023/cc-4298