CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-029

FortiClient Hardcoded Cryptographic Key

June 3, 2020 — v1.0

TLP:WHITE

History:

- *03/06/2020 — v1.0 – Initial publication*

Summary

Fortinet FortiClient for Windows uses a hard-coded cryptographic key to encrypt security sensitive data in the configuration file [1]. The vulnerability allows an attacker with access to the configuration file to disclose sensitive configuration information on the target system. The vulnerability has received CVE number CVE-2019-16150 [1, 3].

Technical Details

The vulnerability, discovered by Gregory Draperi, allows an attacker to disclose sensitive configuration information on the target system. The vulnerability exists due to use of a hard-coded cryptographic key to encrypt the configuration file in FortiClient for Windows. An attacker with access to the configuration (or its backup) can decrypt the file using this default cryptographic key. The vulnerability can also be explited remotely, by an authenticated user of the system, where the configuration file resides [2].

Currently there is no exploit publicly available.

Affected Products

This vulnerability affects Fortinet FortiClient for Windows below 6.4.0.

Recommendations

Upgrade to FortiClient for Windows version 6.4.0 or above.

References

[1] https://www.fortiguard.com/psirt/FG-IR-19-194

[2] https://www.cybersecurity-help.cz/vdb/SB2020060203

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16150