CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-028

FortiClient for Windows Privilege Escalation Vulnerability

May 26, 2020 — v1.0

TLP:WHITE

History:

- *26/05/2020 — v1.0 – Initial publication*

Summary

Fortinet FortiClient for Windows is subject of a local privilege-escalation vulnerability [1]. The vulnerability has received CVE number CVE-2020-9291 [1, 3].

Technical Details

The vulnerability, discovered by Lasse Trolle Borup of Danish Cyber Defence, allows a local user to gain elevated privileges by exhausting the pool of temporary file names combined with a symbolic link attack [2]. This vulnerability can be exploited locally. The attacker should have authentication credentials and successfully authenticate on the system. Currently there is no exploit publicly available.

Affected Products

This vulnerability affects Fortinet FortiClient for Windows version 6.2.1 and earlier.

Recommendations

Upgrade to FortiClient for Windows version 6.2.2 or above.

In case upgrade is not possible, the vulnerability can be mitigated by restricting access to affected computers only to trusted individuals.

References

[1] https://fortiguard.com/psirt/FG-IR-20-040

[2] https://www.cybersecurity-help.cz/vdb/SB2020052615

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9291