Security Advisory 2023-037

High Severity Vulnerability in Cisco AnyConnect Client

June 8, 2023 — v1.0

TLP:CLEAR

History:

- *08/06/2023 — v1.0 – Initial publication*

Summary

On June 7, 2023, Cisco issued an advisory regarding a vulnerability affecting Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows that could allow a low-privileged, authenticated, local attacker to elevate privileges to those of `SYSTEM` [1].

CERT-EU recommends updating the software.

Technical Details

The vulnerability, identified as `CVE-2023-20178` with a CVSS score of 7.8 out of 10, exists because improper permissions are assigned to a temporary directory that is created during the upgrade process. An attacker could exploit this vulnerability by abusing a specific function of the Windows installer process. A successful exploit could allow the attacker to execute code with `SYSTEM` privileges.

Affected Products

- Cisco AnyConnect Secure Mobility Client for Windows Software versions 4.10 and earlier (First Fixed Release is 4.10MR7).
- Cisco Secure Client for Windows Software version 5.0 (First Fixed Release is 4.10MR7).

Recommendations

CERT-EU recommends updating the affected products to the fixed version.

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-csc-privesc-wx4U4Kw