CERT-EU

Security Advisory 2023-030

Sysmon – Local Privilege Escalation Vulnerability

May 15, 2023 — v1.0

TLP:CLEAR

History:

- *15/05/2023 — v1.0 – Initial publication*

Summary

On May 9, 2023, Microsoft disclosed the existence of a Local Privilege Escalation vulnerability in Sysmon. It is identified as **CVE-2023-29343** and could allow an attacker to gain SYSTEM privileges with low attack complexity and without any interaction from a user.

Microsoft currently assesses that the likelihood of exploitation is low due to the lack of a publicly available Proof of Concept exploit, however, it is strongly recommended to update to the latest available Sysmon version [1,2].

Technical Detail

As of the time of writing this advisory, the technical details of this flaw are unknown and an exploit is not yet available.

Products Affected

The vulnerability affects Sysmon products prior to **version 14.16**.

Recommendations

It is highly recommended to update to Sysmon **version 14.16**.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29343

[2] https://arcticwolf.com/resources/blog/cve-2023-29343-sysmon-local-privilege-escalation-vulnerability/