CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-022

Insufficient Access Control Vulnerability in the Dell Driver

May 5, 2021 — v1.0

TLP:WHITE

History:

- 05/05/2021 — v1.0 – Initial publication

Summary

On the 5th of May 2021, Dell has released a security advisory to address multiple vulnerabilities [1]. Those could be exploited by attackers to access driver functions and execute malicious code with kernel-mode privileges.

Technical Details

12-year-old multiple high severity vulnerabilities, tracked as CVE-2021-21551 affect Dell `dbutil` driver. An attacker who gained a foothold in the target system could exploit this bug to escalate privilege and take over it, then perform lateral movement within the target network. Dell has assigned one CVE to cover all the flaws in the firmware update driver, but this single CVE was broken down to the following five separate flaws by SentinelLabs researchers who discovered the issue [2]:

- CVE-2021-21551: Local Elevation Of Privileges #1 – Memory corruption
- CVE-2021-21551: Local Elevation Of Privileges #2 – Memory corruption
- CVE-2021-21551: Local Elevation Of Privileges #3 – Lack of input validation
- CVE-2021-21551: Local Elevation Of Privileges #4 – Lack of input validation
- CVE-2021-21551: Denial Of Service – Code logic issue

SentinelOne reported that they have not seen any indicators of these vulnerabilities being exploited in the wild up till now, but with hundreds of million of enterprises and users currently vulnerable it would change.

Affected Products

These vulnerabilities affects several Dell platforms running Windows operating system. A comprehensive table in Dell advisory details the platforms and software that are impacted by the vulnerable `dbutil_2_3.sys` driver [1].

It is important to note that over the years Dell released BIOS update utilities which contain the vulnerable driver for hundreds of millions of computers (including desktops, laptops, notebooks, and tablets) worldwide.

Recommendations

To fix the issue the vulnerable driver should be removed from the affected system and the latest firmware update utility should be run. Remediation steps are described in detail in [1].

References

[1] https://www.dell.com/support/kbdoc/nl-nl/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability

[2] https://labs.sentinelone.com/cve-2021-21551-hundreds-of-millions-of-dell-computers-at-risk-due-to-multiple-bios-driver-privilege-escalation-flaws/