CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-031

# Critical Vulnerability in DELL BIOSConnect

*June 29, 2021 — v1.0*

**TLP:WHITE**

*History:*

- *29/06/2021 — v1.0 – Initial publication*

## Summary

On 24th of June 2021, Dell released a client platform security update for multiple vulnerabilities in the BIOSConnect and HTTPS Boot features as part of the Dell Client BIOS [1]. The chain of vulnerabilities has a cumulative CVSS score of 8.3 (High) because it allows a privileged network adversary to impersonate `dell.com` and gain arbitrary code execution at the BIOS/UEFI level of the affected device. This would enable adversaries to control the device's boot process and subvert the operating system and higher-layer security controls [2].

## Technical Details

### CVE-2021-21571 - CVSS 5.9

Dell UEFI BIOS HTTPS stack leveraged by the Dell BIOSConnect feature and Dell HTTPS Boot feature contains an improper certificate validation vulnerability. A remote unauthenticated attacker may exploit this vulnerability using a person-in-the-middle attack, which may lead to a denial of service and payload tampering.

### CVE-2021-21572, CVE-2021-21573, CVE-2021-21574 - CVSS 7.2

Dell BIOSConnect feature contains a buffer overflow vulnerability. An authenticated malicious admin user with local access to the system may potentially exploit this vulnerability to run arbitrary code and bypass UEFI restrictions.

To exploit the vulnerabilities in BIOSConnect or HTTPS Boot, a malicious actor must separately perform additional steps before a successful exploit, including: compromise a user's network, obtain a certificate that is trusted by one of the Dell UEFI BIOS HTTPS stack's built-in Certificate Authorities, and wait for a user who is physically present at the system to use the BIOSConnect feature or to change the boot order and use the HTTPS Boot feature.

## Products Affected

CVE-2021-21573 and CVE-2021-21574 were remediated on the server side since May 28, 2021 and require no additional customer action.

CVE-2021-21571 and CVE-2021-21572 require Dell Client BIOS updates to address the vulnerabilities. These vulnerabilities affects 129 Dell models of consumer and business laptops, desktops, and tablets, including devices protected by Secure Boot and Dell Secured-core PCs. The full list of the affected models can be found in [1].

## Recommendations

CERT-EU recommends updating the vulnerable application as soon as possible using the patches listed in [1].

### Workarounds and Mitigations

For those that cannot apply BIOS updates immediately, Dell has also provided an interim mitigation to disable the BIOSConnect and HTTPS Boot features [1].

## References

[1] https://www.dell.com/support/kbdoc/fr-be/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-biosconnect-feature-and-https-boot-feature

[2] https://eclypsium.com/2021/06/24/biosdisconnect/