Eclypsium Discovers Multiple Vulnerabilities Affecting 128 Dell Models via Dell Remote OS Recovery and Firmware Update Capabilities

BIOS Disconnect - Vendor Update Tools Pose Significant Risks to the Integrity of Dell Devices

INTRODUCTION

Eclypsium researchers have identified multiple vulnerabilities affecting the BIOSConnect feature within Dell Client BIOS. This 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. Such an attack would enable adversaries to control the device's boot process and subvert the operating system and higher-layer security controls. The issue affects 128 Dell models of consumer and business laptops, desktops, and tablets, including devices protected by Secure Boot and Dell Secured-core PCs.

The Eclypsium team has coordinated with Dell PSIRT throughout the disclosure process. Dell has issued a Dell Security Advisory and is scheduling BIOS/UEFI updates for affected systems and updates to affected executables from Dell.com. Please reference the Mitigations section for the latest information on how to protect affected devices.

These vulnerabilities enable an attacker to remotely execute code in the pre-boot environment. Such code may alter the initial state of an operating system, violating common assumptions on the hardware/firmware layers and breaking OS-level security controls. As attackers increasingly shift their focus to vendor supply chains and system firmware, it is more important than ever that organizations have independent visibility and control over the integrity of their devices.

BACKGROUND

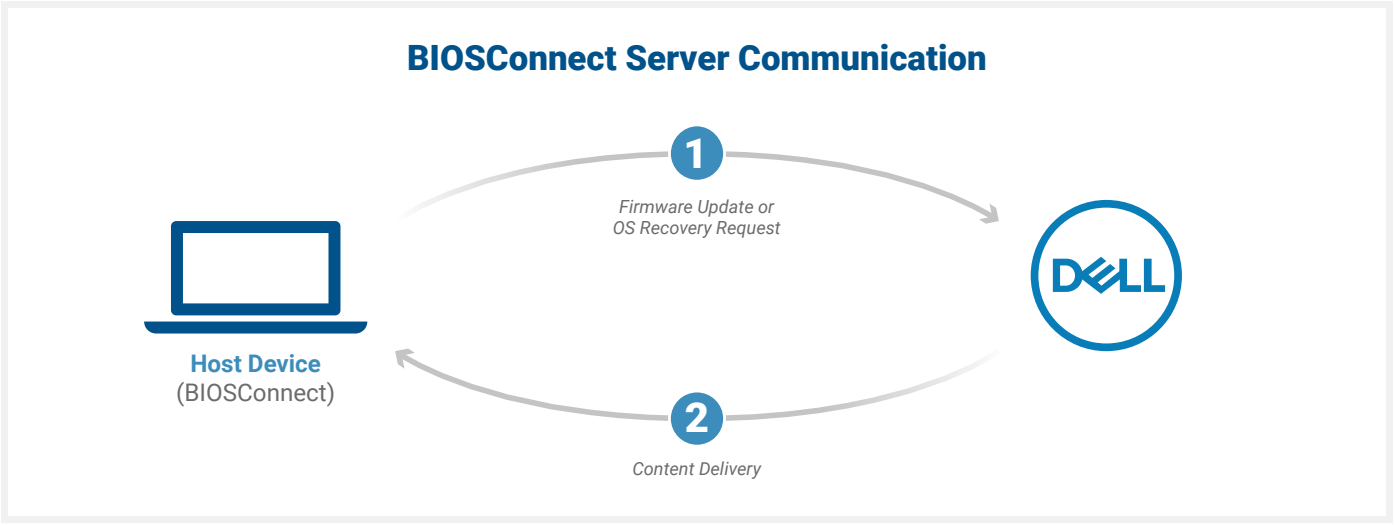
Dell SupportAssist is an overarching support solution that comes preinstalled on most Windows-based Dell machines. SupportAssist covers a range of support functions such as monitoring for hardware and software problems and assisting with troubleshooting and recovery when issues are found.

BIOSConnect is a feature of SupportAssist that allows users to perform a remote OS recovery or update the firmware on the device. In either case (firmware update or OS recovery), BIOSConnect enables the system's BIOS to reach out to Dell backend services over the Internet and then coordinate the update or recovery process. Dell describes BIOSConnect as follows:

"BIOSConnect provides a foundation platform allowing BIOS to connect to a Dell HTTPs backend and load an image via https method. This foundation expands the Serviceability feature set to enhance the on-box reliability experience by adding cloud-based Service OS (SOS) support.

BIOSConnect feature offers network-based SOS boot recovery capability by performing HTTP(s) download from the cloud to a local RAMDisk and transfers control to the downloaded Service OS image to perform the necessary corrective action. This enables the user to recover when the local HDD image is corrupted, replaced, or absent."

The details vary between the firmware update and OS recovery processes, but the high-level operation is the same -- BIOSConnect connects to Dell's update infrastructure, and Dell delivers content needed to update or recover some of the most sensitive code on the device.



VULNERABILITY OVERVIEW & ATTACK SCENARIO

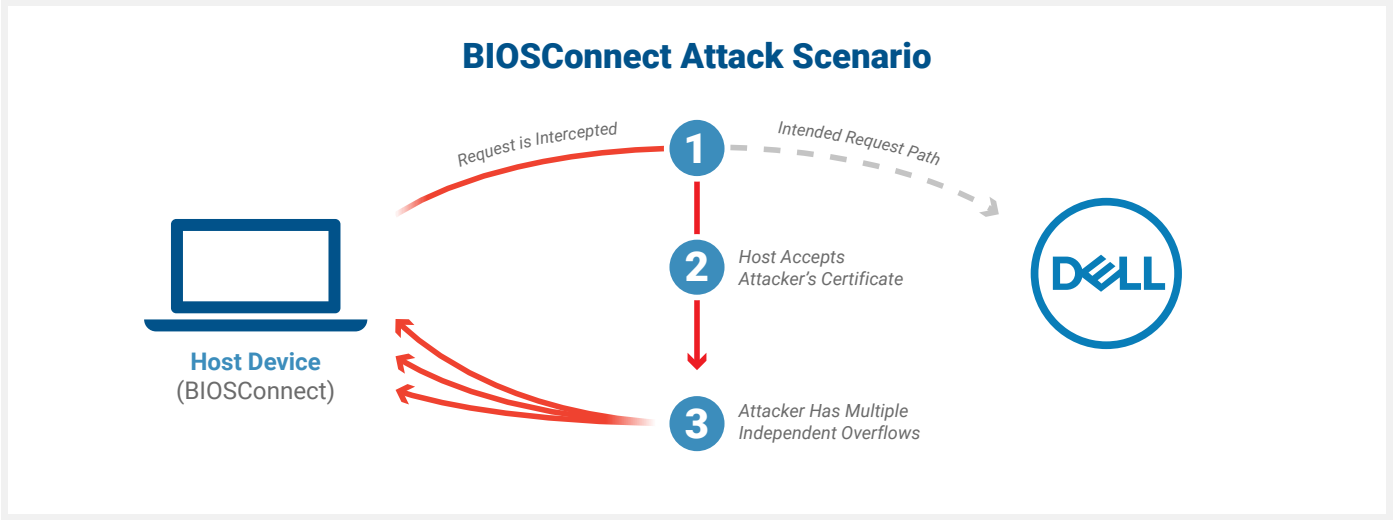
Our research has identified a series of four vulnerabilities that would enable a privileged network attacker to gain arbitrary code execution within the BIOS of vulnerable machines. The vulnerabilities were originally discovered on a Dell Secured-core PC Latitude 5310 using Secure Boot, and we later confirmed the issue on other models of desktops and laptops.

1. **Insecure TLS Connection from BIOS to Dell** - CVE-2021-21571. When attempting to connect to the backend Dell HTTP server, the TLS connection from BIOSConnect will accept any valid wildcard certificate. This allows an attacker with a privileged network position to impersonate Dell and deliver attacker-controlled content back to the victim device.

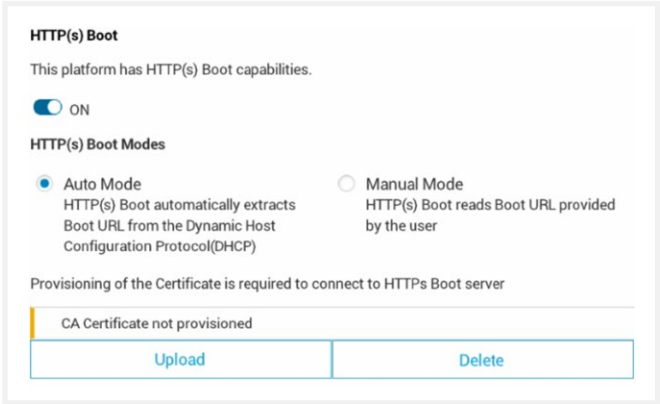
   The process of verifying the certificate for dell.com is done by first retrieving the DNS record from the hard-coded server 8.8.8.8 (Google) then establishing a connection to https://downloads.dell.com. However, any valid wildcard certificate issued by any of the built-in CA's contained within the BIOSConnect feature in BIOS will satisfy the secure connection condition, and BIOSConnect will proceed to retrieve the relevant files. The bundle of CA root certificates in the BIOS image was sourced from Mozilla's root certificate file (certdata.txt).

   When UEFI Secure Boot is disabled, this vulnerability can be used to gain arbitrary remote code execution in the UEFI/pre-boot environment on the client device without needing to take advantage of the additional buffer overflow vulnerabilities.

   1.1. **Vulnerable HTTPS Boot configurations** - Some HTTPS Boot configurations may also be exploitable due to using the same underlying verification code. When configuring HTTPS Boot, the user is required to provision a Certificate Authority (CA) certificate, which is intended to



be used to verify connections to the remote boot server before allowing the HTTP Boot process to proceed. However, when this verification is performed, any valid certificate for any domain acquired from the same CA will be accepted, not just those for the configured remote boot server. Due to this limitation, CAs that issue certificates broadly (commercial, non-profit, cloud, web hosting etc.) should not be used for this role.



2. **Overflow Vulnerabilities Enabling Arbitrary Code Execution** - With the ability to impersonate Dell, the attacker can deliver malicious content back to the victim machine. Through subsequent analysis, we have identified three overflow vulnerabilities, CVE-2021-21572, CVE-2021-21573, CVE-2021-21574. Two of these vulnerabilities affect the OS recovery process, while the other affects the firmware update process. All three vulnerabilities are independent, and each one could lead to arbitrary code execution in BIOS. Eclypsium will release additional detailed analyses of each vulnerability in August at DEF CON.

As noted above, an attack scenario would require an attacker to be able to redirect the victim's traffic, such as via a Machine-in-the-Middle (MITM) attack. However, the virtually unlimited control over a device that this attack can provide makes it worth the effort by the attacker.

First, recent attacks have highlighted the great length that attackers will go to in order to compromise a vendor's supply chain and support infrastructure. Machine-in-the-Middle attacks are a relatively low bar to sophisticated attackers, with techniques such as ARP spoofing and DNS cache poisoning being well-known and easily automated. Additionally, enterprise VPNs and other network devices have become a top target of attackers, and flaws in these devices can allow attackers to redirect traffic. And finally, end-users working from home are increasingly reliant on SOHO networking gear. Vulnerabilities are quite common in these types of consumer-grade networking devices and have been exploited in widespread campaigns.

Successfully compromising the BIOS of a device would give an attacker a high degree of control over a device. The attacker could control the process of loading the host operating system and disable protections in order to remain undetected. This would allow an attacker to establish ongoing persistence while controlling the highest privileges on the device.

SCOPE

The problem affects 128 different models of Dell laptops, tablets, and desktops, and an estimated 30 million individual devices. As described earlier, the issue has been found on Secured-core PCs even if Secure Boot is enabled.

Please see Dell's advisory for the full list of affected models.

MITIGATIONS

The system BIOS/UEFI will need to be updated for all affected systems. However, we recommend that users not use BIOSConnect to perform this firmware update. Instead, it is advisable to run the BIOS update executable from the OS after manually checking the hashes against those published by Dell.

Dell will be updating the affected executables delivered during the BIOSConnect firmware update and OS recovery processes. According to Dell, two of the vulnerabilities have been remediated on the server side, with additional updates coming in July. We will update this blog as they become available.

Dell has posted an advisory and provided the following recommended mitigations and workarounds:

> **"Affected Products and Remediation**
>
> CVE-2021-21573, CVE-2021-21574 were remediated on the server side on May 28, 2021 and require no additional customer action.
>
> CVE-2021-21571, CVE-2021-21572 require Dell Client BIOS updates to address the vulnerabilities. Refer to the table under the Additional Information section to determine the version of the remediated Dell Client BIOS to apply to your system. There are multiple ways to update your Dell Client BIOS. If you typically use BIOSConnect to update your BIOS, Dell recommends using a different method to apply the BIOS updates, such as:
>
> - Using one of the Dell notification solutions to be notified and download BIOS updates automatically once available.
> - Visiting the Drivers and Downloads site for updates on the applicable products. To learn more, visit the Dell Knowledge Base article Dell BIOS Updates, and download the update for your Dell computer.
> - Flashing the BIOS from the F12 One-Time Boot Menu.
>
> For those that cannot apply BIOS updates immediately, Dell has also provided an interim mitigation to disable the BIOSConnect and HTTPS Boot features. See the following section.
>
> **Workaround and Mitigations**
>
> Dell recommends all customers update to the latest Dell Client BIOS version at the earliest opportunity. Customers who choose not to apply BIOS updates immediately or who are otherwise unable to do so at this time should apply the below mitigation.
>
> **BIOSConnect:**
>
> Customers may disable the BIOSConnect feature using one of two options:
>
> Option 1: Customers may disable BIOSConnect from the BIOS setup page (F2).
>
> *Note: Customers may find the BIOSConnect option under different BIOS setup menu interfaces depending on their platform model. These are referred below as BIOS Setup Menu Type A and BIOS Setup Menu Type B.*
>
> BIOS Setup Menu Type A: F2-> Update,Recovery -> BIOSConnect -> Switch to Off
>
> BIOS Setup Menu Type B: F2 -> Settings -> SupportAssist System Resolution -> BIOSConnect -> Uncheck BIOSConnect option
>
> *Note: Dell recommends customers not to run "BIOS Flash Update - Remote" from F12 until the system is updated with a remediated version of the BIOS.*
>
> Option 2: Customers may leverage Dell Command | Configure (DCC)'s Remote System Management tool to disable the BIOSConnect and Firmware Over the Air (FOTA) BIOS settings.
>
> **HTTPS Boot:**
>
> Customers may disable the HTTPS Boot feature using one of two options:
>
> Option 1: Customers may disable BIOSConnect from the BIOS setup page (F2).
>
> F2-> Connection -> HTTP(s) Boot -> Switch to Off
>
> BIOS Setup Menu Type B: F2 -> Settings -> SupportAssist System Resolution -> BIOSConnect -> Uncheck BIOSConnect option
>
> Option 2: Customers may leverage Dell Command | Configure (DCC)'s Remote System Management tool to disable HTTP Boot Support."

The Eclypsium platform has functionality to detect these vulnerabilities, allowing organizations to quickly and easily discover all affected devices in their environments. Additionally, Eclypsium can assist with the firmware update process to ensure that all firmware updates are valid.

CONCLUSION

Technology vendors of all types are increasingly implementing over-the-air update processes to make it as easy as possible for their customers to keep their firmware up to date and recover from system failures. And while this is a valuable option, any vulnerabilities in these processes, such as those we've seen here in Dell's BIOSConnect can have serious consequences. The specific vulnerabilities covered here allow an attacker to remotely exploit the UEFI firmware of a host and gain control over the most privileged code on the device. This combination of remote exploitability and high privileges will likely make remote update functionality an alluring target for attackers in the future, and organizations should make sure to monitor and update their devices accordingly.

We will continue to update this blog with additional detailed analysis from the Eclypsium team and updates from Dell as they become available.

TIMELINE

March 2 Initial issues discovered by Eclypsium

March 3 Dell PSIRT notified, acknowledges receipt

May 14 Dell PSIRT proposes a plan to remediate 2 of the issues by June with additional updates by the end of July

June 24 Eclypsium blog and Dell disclosure released

Aug 5-8 Eclypsium will provide a technical deep-dive with additional details for the four vulnerabilities at DEF CON