Article Number: 000188682

Print Email English Alert

DSA-2021-106: Dell Client Platform Security Update for Multiple Vulnerabilities in the BIOSConnect and HTTPS Boot features as part of the Dell Client BIOS

Summary: Dell is releasing remediations for multiple security vulnerabilities affecting the BIOSConnect and HTTPS Boot features.

Article Content

Impact

High

Details

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2021-21571	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.	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:H
CVE-2021-21572, CVE-2021-21573, CVE-2021-21574	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.	7.2	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

Description of the Dell BIOSConnect and HTTPS Boot features:

ARTICLE CONTENT
LEGAL INFORMATION
ARTICLE PROPERTIES
RATE THIS ARTICLE

Contact Us

- The Dell BIOSConnect feature is a Dell preboot solution that is used to update system BIOS and recover the operating system (OS) using the SupportAssist OS Recovery on Dell Client platforms. Note: BIOSConnect requires a physically present user to initiate this feature. Only a subset of platforms with the BIOSConnect feature is affected. See the table under Additional Information section below for impacted platforms.
- The Dell HTTPS Boot feature is an extension to UEFI HTTP Boot specifications to boot from an HTTP(S) Server. Note: This feature is not configured by default and requires a physically present user with local OS admin rights to configure. Additionally, a physically present user is required to initiate the feature when used with wireless networks. Not all platforms contain the HTTPS Boot feature. See the table under the Additional Information section below for a list of impacted platforms.

The above vulnerabilities were reported as a vulnerability chain. The cumulative score of the vulnerability chain is: 8.3 High CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H.

Exploiting the chain requires additional steps:

- To exploit the vulnerability chain in BIOSConnect, 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.
- To exploit the vulnerability in 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 change the boot order and use the HTTPS Boot feature.

In addition to applying the remediations below, customers can further protect themselves by following security best practices by only using secured networks and preventing unauthorized local and physical access to devices. Customers should also enable platform security features such as Secure Boot (enabled by default for Dell platforms with Windows) and BIOS Admin Password for added protection.

Note: If Secure Boot is disabled, it may impact the potential severity that is associated with the CVE-2021-21571 security vulnerability.

> Dell Technologies recommends all customers consider both the CVSS base score and any relevant temporal and environmental scores that may impact the potential severity associated with a particular security vulnerability.

Affected Products and Remediation

CVE-2021-21573 and CVE-2021-21574 were remediated in the BIOSConnect related components on Dell back-end servers on 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. See 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 section below.

Workarounds and Mitigations

ARTICLE CONTENT

LEGAL INFORMATION

ARTICLE PROPERTIES

RATE THIS ARTICLE

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 now, 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 seen 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.

  Option 2: Customers may leverage Dell Command | Configure (DCC)’s Remote System Management tool to disable the BIOSConnect BIOS settings.

  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.

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.

Acknowledgements

Dell would like to thank Mickey Shkatov and Jesse Michael of Eclypsium for reporting this issue.

Revision History

Revision	Date	Description
1.0	2021-06-24	Initial Release

Related Information

Dell Security Advisories and Notices
Dell Vulnerability Response Policy
CVSS Scoring Guide

Additional Information

The following is a list of impacted products and release dates and minimal BIOS versions to apply:

Product	BIOS Update Version (or greater)	Supports BIOSConnect	Supports HTTP(s) Boot	Release Date (MM/DD/YYYY) Expected Release (Month /YYYY)
Alienware m15 R6	1.3.3	Yes	Yes	6/21/2021

Contact Us

AI
LEGA
ARTI
RA

Contact Us

ChengMing 3990	1.4.1	Yes	No	6/23/2021
ChengMing 3991	1.4.1	Yes	No	6/23/2021
Dell G15 5510	1.4.0	Yes	Yes	6/21/2021
Dell G15 5511	1.3.3	Yes	Yes	6/21/2021
Dell G3 3500	1.9.0	Yes	No	6/24/2021
Dell G5 5500	1.9.0	Yes	No	6/24/2021
Dell G7 7500	1.9.0	Yes	No	6/23/2021
Dell G7 7700	1.9.0	Yes	No	6/23/2021
Inspiron 14 5418	2.1.0 A06	Yes	Yes	6/24/2021
Inspiron 15 5518	2.1.0 A06	Yes	Yes	6/24/2021
Inspiron 15 7510	1.0.4	Yes	Yes	6/23/2021
Inspiron 3501	1.6.0	Yes	No	6/23/2021
Inspiron 3880	1.4.1	Yes	No	6/23/2021
Inspiron 3881	1.4.1	Yes	No	6/23/2021
Inspiron 3891	1.0.11	Yes	Yes	6/24/2021
Inspiron 5300	1.7.1	Yes	No	6/23/2021
Inspiron 5301	1.8.1	Yes	No	6/23/2021
Inspiron 5310	2.1.0	Yes	Yes	6/23/2021
Inspiron 5400 2n1	1.7.0	Yes	No	6/23/2021
Inspiron 5400 AIO	1.4.0	Yes	No	6/23/2021
Inspiron 5401	1.7.2	Yes	No	6/23/2021
Inspiron 5401 AIO	1.4.0	Yes	No	6/23/2021
Inspiron 5402	1.5.1	Yes	No	6/23/2021
Inspiron 5406 2n1	1.5.1	Yes	No	6/23/2021
Inspiron 5408	1.7.2	Yes	No	6/23/2021
Inspiron 5409	1.5.1	Yes	No	6/23/2021

AI

LEGA

ARTI

RA

Inspiron 5410 2-in-1	2.1.0	Yes	Yes	6/23/2021
Inspiron 5501	1.7.2	Yes	No	6/23/2021
Inspiron 5502	1.5.1	Yes	No	6/23/2021
Inspiron 5508	1.7.2	Yes	No	6/23/2021
Inspiron 5509	1.5.1	Yes	No	6/23/2021
Inspiron 7300	1.8.1	Yes	No	6/23/2021
Inspiron 7300 2n1	1.3.0	Yes	No	6/23/2021
Inspiron 7306 2n1	1.5.1	Yes	No	6/23/2021
Inspiron 7400	1.8.1	Yes	No	6/23/2021
Inspiron 7500	1.8.0	Yes	No	6/23/2021
Inspiron 7500 2n1 - Black	1.3.0	Yes	No	6/23/2021
Inspiron 7500 2n1 - Silver	1.3.0	Yes	No	6/23/2021
Inspiron 7501	1.8.0	Yes	No	6/23/2021
Inspiron 7506 2n1	1.5.1	Yes	No	6/23/2021
Inspiron 7610	1.0.4	Yes	Yes	6/23/2021
Inspiron 7700 AIO	1.4.0	Yes	No	6/23/2021
Inspiron 7706 2n1	1.5.1	Yes	No	6/23/2021
Latitude 3120	1.1.0	Yes	No	6/23/2021
Latitude 3320	1.4.0	Yes	Yes	6/23/2021
Latitude 3410	1.9.0	Yes	No	6/23/2021
Latitude 3420	1.8.0	Yes	No	6/23/2021
Latitude 3510	1.9.0	Yes	No	6/23/2021
Latitude 3520	1.8.0	Yes	No	6/23/2021
Latitude 5310	1.7.0	Yes	No	6/24/2021

Contact Us

AI
LEGA
ARTI
RA
Contact Us

Latitude 5310 2 in 1	1.7.0	Yes	No	6/24/2021
Latitude 5320	1.7.1	Yes	Yes	6/21/2021
Latitude 5320 2-in-1	1.7.1	Yes	Yes	6/21/2021
Latitude 5410	1.6.0	Yes	No	6/23/2021
Latitude 5411	1.6.0	Yes	No	6/23/2021
Latitude 5420	1.8.0	Yes	Yes	6/22/2021
Latitude 5510	1.6.0	Yes	No	6/23/2021
Latitude 5511	1.6.0	Yes	No	6/23/2021
Latitude 5520	1.7.1	Yes	Yes	6/21/2021
Latitude 5521	1.3.0 A03	Yes	Yes	6/22/2021
Latitude 7210 2-in-1	1.7.0	Yes	No	6/23/2021
Latitude 7310	1.7.0	Yes	No	6/23/2021
Latitude 7320	1.7.1	Yes	Yes	6/23/2021
Latitude 7320 Detachable	1.4.0 A04	Yes	Yes	6/22/2021
Latitude 7410	1.7.0	Yes	No	6/23/2021
Latitude 7420	1.7.1	Yes	Yes	6/23/2021
Latitude 7520	1.7.1	Yes	Yes	6/23/2021
Latitude 9410	1.7.0	Yes	No	6/23/2021
Latitude 9420	1.4.1	Yes	Yes	6/23/2021
Latitude 9510	1.6.0	Yes	No	6/23/2021
Latitude 9520	1.5.2	Yes	Yes	6/23/2021
Latitude 5421	1.3.0 A03	Yes	Yes	6/22/2021
OptiPlex 3080	2.1.1	Yes	No	6/23/2021
OptiPlex 3090 UFF	1.2.0	Yes	Yes	6/23/2021
OptiPlex 3280 All-in-One	1.7.0	Yes	No	6/23/2021

AI
LEGA
ARTI
RA
Contact Us

OptiPlex 5080	1.4.0	Yes	No	6/23/2021
OptiPlex 5090 Tower	1.1.35	Yes	Yes	6/23/2021
OptiPlex 5490 AIO	1.3.0	Yes	Yes	6/24/2021
OptiPlex 7080	1.4.0	Yes	No	6/23/2021
OptiPlex 7090 Tower	1.1.35	Yes	Yes	6/23/2021
OptiPlex 7090 UFF	1.2.0	Yes	Yes	6/23/2021
OptiPlex 7480 All-in-One	1.7.0	Yes	No	6/23/2021
OptiPlex 7490 All-in-One	1.3.0	Yes	Yes	6/24/2021
OptiPlex 7780 All-in-One	1.7.0	Yes	No	6/23/2021
Precision 17 M5750	1.8.2	Yes	No	6/9/2021
Precision 3440	1.4.0	Yes	No	6/23/2021
Precision 3450	1.1.35	Yes	Yes	6/24/2021
Precision 3550	1.6.0	Yes	No	6/23/2021
Precision 3551	1.6.0	Yes	No	6/23/2021
Precision 3560	1.7.1	Yes	Yes	6/21/2021
Precision 3561	1.3.0 A03	Yes	Yes	6/22/2021
Precision 3640	1.6.2	Yes	No	6/23/2021
Precision 3650 MT	1.2.0	Yes	Yes	6/24/2021
Precision 5550	1.8.1	Yes	No	6/23/2021
Precision 5560	1.3.2	Yes	Yes	6/23/2021
Precision 5760	1.1.3	Yes	Yes	6/16/2021
Precision 7550	1.8.0	Yes	No	6/23/2021
Precision 7560	1.1.2	Yes	Yes	6/22/2021
Precision 7750	1.8.0	Yes	No	6/23/2021

AI
LEGA
ARTI
RA

Contact Us

Precision 7760	1.1.2	Yes	Yes	6/22/2021
Vostro 14 5410	2.1.0 A06	Yes	Yes	6/24/2021
Vostro 15 5510	2.1.0 A06	Yes	Yes	6/24/2021
Vostro 15 7510	1.0.4	Yes	Yes	6/23/2021
Vostro 3400	1.6.0	Yes	No	6/23/2021
Vostro 3500	1.6.0	Yes	No	6/23/2021
Vostro 3501	1.6.0	Yes	No	6/23/2021
Vostro 3681	2.4.0	Yes	No	6/23/2021
Vostro 3690	1.0.11	Yes	Yes	6/24/2021
Vostro 3881	2.4.0	Yes	No	6/23/2021
Vostro 3888	2.4.0	Yes	No	6/23/2021
Vostro 3890	1.0.11	Yes	Yes	6/24/2021
Vostro 5300	1.7.1	Yes	No	6/23/2021
Vostro 5301	1.8.1	Yes	No	6/23/2021
Vostro 5310	2.1.0	Yes	Yes	6/23/2021
Vostro 5401	1.7.2	Yes	No	6/23/2021
Vostro 5402	1.5.1	Yes	No	6/23/2021
Vostro 5501	1.7.2	Yes	No	6/23/2021
Vostro 5502	1.5.1	Yes	No	6/23/2021
Vostro 5880	1.4.0	Yes	No	6/23/2021
Vostro 5890	1.0.11	Yes	Yes	6/24/2021
Vostro 7500	1.8.0	Yes	No	6/23/2021
XPS 13 9305	1.0.8	Yes	No	6/23/2021
XPS 13 2in1 9310	2.3.3	Yes	No	6/23/2021
XPS 13 9310	3.0.0	Yes	No	6/24/2021
XPS 15 9500	1.8.1	Yes	No	6/23/2021
XPS 15 9510	1.3.2	Yes	Yes	6/23/2021

AF
LEGA
ARTICLE PROPERTIES
RATE THIS ARTICLE

XPS 17 9700	1.8.2	Yes	No	6/9/2021
XPS 17 9710	1.1.3	Yes	Yes	6/15/2021

Legal Information

The information in this Dell Technologies Security Advisory should be read and used to assist in avoiding situations that may arise from the problems described herein. Dell Technologies distributes Security Advisories to bring important security information to the attention of users of the affected product(s). Dell Technologies assesses the risk based on an average of risks across a diverse set of installed systems and may not represent the actual risk to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. The information set forth herein is provided "as is" without warranty of any kind. Dell Technologies expressly disclaims all warranties, either express or implied, including the warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation shall apply to the extent permissible under law.

Contact Us

Article Properties

Affected Product

Alienware m15 R6, Inspiron, OptiPlex, Latitude, Vostro, XPS

Product

Product Security Information

Last Published Date

01 Jul 2021

Version

4

Article Type

Dell Security Advisory

Rate This Article

Accurate

Useful

AI

LEG/

ARTI

RA

Easy to Understand

Was this article helpful?

○ Yes ○ No

Additional Information (optional)

0/3000 characters

Submit Feedback

Contact Us

Your Recently Viewed Articles

[Supported Platforms/BIOS reference list for Dell Command Configure, Dell Command Monitor, and Dell Command PowerShell Provider]

About Dell Technologies Careers Community Events Partner Program

Premier Find a Reseller Dell Technologies Make a Payment

United States

Terms of Sale Privacy Statement Ads & Emails Legal & Regulatory Social Impact Product Recycling

Anti-Slavery & Human Trafficking Contact Us Site Map