DSA-2022-186: Dell Client Security Update for Dell Client BIOS

Summary: Dell Client Consumer and Commercial platform remediation is available for this vulnerability that may be exploited by malicious users to compromise the affected systems.

Impact

Medium

Details

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2022-29083	Dell BIOS versions before the ones listed in the table below contain an Improper Authentication vulnerability. An unauthenticated attacker with physical access to the system may potentially exploit this vulnerability by bypassing drive security mechanisms in order to gain access to the system.	6.8	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

See the table below for Dell Client BIOS releases containing resolutions to these vulnerabilities. Dell recommends all customers update at the earliest opportunity.

Go to the Drivers and Downloads site for updates on the applicable products. To learn more, see Dell article 124211, Dell BIOS Updates, and download the update for your Dell computer.

Customers may use one of the Dell notification solutions to be notified and download driver, BIOS, and firmware updates automatically once available.

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2022-29083	Dell BIOS versions before the ones listed in the table below contain an Improper Authentication vulnerability. An unauthenticated attacker with physical access to the system may potentially exploit this vulnerability by bypassing drive security mechanisms in order to gain access to the system.	6.8	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

See the table below for Dell Client BIOS releases containing resolutions to these vulnerabilities. Dell recommends all customers update at the earliest opportunity.

Go to the Drivers and Downloads site for updates on the applicable products. To learn more, see Dell article 124211, Dell BIOS Updates, and download the update for your Dell computer.

Customers may use one of the Dell notification solutions to be notified and download driver, BIOS, and firmware updates automatically once available.

⚠ 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 & Remediation

Product	BIOS Update Version	BIOS Release Date (MM/DD/YYYY)
ChengMing 3980	2.23.0	05/09/2022
ChengMing 3990	1.11.0	05/09/2022
ChengMing 3991	1.11.0	05/09/2022
Dell G3 3579	1.21.0	05/10/2022

Dell G3 3779	1.21.0	05/10/2022
Dell G5 15 5587	1.21.0	05/10/2022
Dell G5 5000	1.7.0	05/11/2022
Dell G5 5090	1.14.0	05/19/2022
Dell G7 15 7588	1.21.0	05/10/2022
Inspiron 3470	2.23.0	05/09/2022
Inspiron 3480	1.19.0	05/10/2022
Inspiron 3493	1.19.0	01/13/2022
Inspiron 3501	1.11.0	01/13/2022
Inspiron 3580	1.19.0	05/10/2022
Inspiron 3580	1.19.0	05/10/2022
Inspiron 3593	1.19.0	01/13/2022
Inspiron 3670	2.23.0	05/10/2022
Inspiron 3780	1.19.0	05/10/2022
Inspiron 3790	1.16.0	01/12/2022
Inspiron 3793	1.19.0	01/13/2022
Inspiron 3880	1.11.0	05/09/2022
Inspiron 3881	1.11.0	05/10/2022
Inspiron 5310	2.6.1	12/09/2021
Inspiron 5410 2-in-1	2.6.1	01/11/2022
Inspiron 5493	1.19.0	01/13/2022
Inspiron 5494	1.16.0	01/12/2022
Inspiron 5510	2.6.1	01/11/2022
Inspiron 5593	1.19.0	01/13/2022
Inspiron 5594	1.16.0	01/12/2022
Inspiron 7490	1.11.0	01/13/2022

Inspiron 7510	1.4.0	01/07/2022
Inspiron 7610	1.4.0	01/07/2022
Latitude 3120	1.9.2	07/04/2022
Latitude 3190	1.21.1	07/06/2022
Latitude 3190 2-In-1	1.21.1	07/06/2022
Latitude 3320	1.8.2	12/09/2021
Latitude 5310	1.9.1	10/26/2022
Latitude 5310 2-in-1	1.9.1	10/26/2022
Latitude 5410	1.8.1	11/11/2021
Latitude 5411	1.8.1	11/09/2021
Latitude 5491	1.21.1	06/23/2022
Latitude 5510	1.8.1	11/11/2021
Latitude 5511	1.8.1	11/09/2021
Latitude 5591	1.21.1	06/23/2022
Latitude 7210 2-in-1	1.9.1	11/11/2021
Latitude 7310	1.9.1	11/10/2021
Latitude 7410	1.9.1	11/10/2021
Latitude 9410	1.9.1	11/10/2021
Latitude 9510	1.8.1	11/10/2021
OptiPlex 3060	1.20.0	06/15/2022
OptiPlex 3070	1.15.0	06/15/2022
OptiPlex 3080	2.11.0	05/11/2022
OptiPlex 3090	2.4.0	05/11/2022
OptiPlex 5060	1.20.0	06/15/2022
OptiPlex 5070	1.15.0	06/15/2022
OptiPlex 5080	1.11.0	05/11/2022

OptiPlex 5260 All-In-One	1.20.1	06/16/2022
OptiPlex 5270 All-in-One	1.15.1	06/15/2022
OptiPlex 7060	1.20.0	06/15/2022
OptiPlex 7070	1.15.0	06/15/2022
OptiPlex 7070 Ultra	1.13.2	06/08/2022
OptiPlex 7071	1.14.1	06/14/2022
OptiPlex 7080	1.11.0	05/10/2022
OptiPlex 7460 All-In-One	1.20.1	06/15/2022
OptiPlex 7470 All-in-One	1.15.1	06/15/2022
OptiPlex 7760 All-In-One	1.20.1	06/15/2022
OptiPlex 7770 All-in-One	1.15.1	06/15/2022
OptiPlex XE3	1.20.0	06/15/2022
Precision 3240 Compact	1.12.0	07/07/2022
Precision 3430 Tower	1.19.0	05/09/2022
Precision 3431 Tower	1.14.0	05/09/2022
Precision 3440	1.11.0	05/09/2022
Precision 3530	1.21.1	06/23/2022
Precision 3550	1.8.1	11/11/2021
Precision 3551	1.8.1	11/09/2021
Precision 3630 Tower	2.14.1	06/16/2022
Precision 3640 Tower	1.15.0	07/05/2022
Precision 3650 Tower	1.7.0	01/12/2022
Precision 3930 Rack	2.19.2	06/07/2022
Precision 7530	1.22.1	06/23/2022
Precision 7540	1.20.2	06/23/2022
Precision 7550	1.10.1	11/09/2021

Precision 7730	1.22.1	06/23/2022
Precision 7740	1.20.2	06/23/2022
Precision 7750	1.10.1	11/09/2021
Vostro 15 7580	1.21.0	05/10/2022
Vostro 3070	2.23.0	05/10/2022
Vostro 3401	1.11.0	01/13/2022
Vostro 3470	2.23.0	05/09/2022
Vostro 3480	1.19.0	05/10/2022
Vostro 3490	1.16.0	01/12/2022
Vostro 3501	1.11.0	01/13/2022
Vostro 3580	1.19.0	05/10/2022
Vostro 3583	1.19.0	05/10/2022
Vostro 3590	1.16.0	01/12/2022
Vostro 3670	2.23.0	05/10/2022
Vostro 3681	2.11.0	05/09/2022
Vostro 3881	2.11.0	05/09/2022
Vostro 3888	2.11.0	05/09/2022
Vostro 5090	1.14.0	05/10/2022
Vostro 5310	2.6.1	12/09/2021
Vostro 5410	2.6.1	01/11/2022
Vostro 5491	1.19.0	01/13/2022
Vostro 5510	2.6.1	01/11/2022
Vostro 5591	1.19.0	01/13/2022
Vostro 5880	1.11.0	05/10/2022
Vostro 7510	1.4.0	01/07/2022
Wyse 5070	1.17.0	05/10/2022

Wyse 5470	1.14.0	05/10/2022
Wyse 5470 All-In-One	1.15.0	05/10/2022
XPS 8940	2.6.0	05/11/2022

Product	BIOS Update Version	BIOS Release Date (MM/DD/YYYY)
ChengMing 3980	2.23.0	05/09/2022
ChengMing 3990	1.11.0	05/09/2022
ChengMing 3991	1.11.0	05/09/2022
Dell G3 3579	1.21.0	05/10/2022
Dell G3 3779	1.21.0	05/10/2022
Dell G5 15 5587	1.21.0	05/10/2022
Dell G5 5000	1.7.0	05/11/2022
Dell G5 5090	1.14.0	05/19/2022
Dell G7 15 7588	1.21.0	05/10/2022
Inspiron 3470	2.23.0	05/09/2022
Inspiron 3480	1.19.0	05/10/2022
Inspiron 3493	1.19.0	01/13/2022
Inspiron 3501	1.11.0	01/13/2022
Inspiron 3580	1.19.0	05/10/2022
Inspiron 3580	1.19.0	05/10/2022
Inspiron 3593	1.19.0	01/13/2022
Inspiron 3670	2.23.0	05/10/2022
Inspiron 3780	1.19.0	05/10/2022
Inspiron 3790	1.16.0	01/12/2022
Inspiron 3793	1.19.0	01/13/2022
Inspiron 3880	1.11.0	05/09/2022
Inspiron 3881	1.11.0	05/10/2022

Inspiron 5310	2.6.1	12/09/2021
Inspiron 5410 2-in-1	2.6.1	01/11/2022
Inspiron 5493	1.19.0	01/13/2022
Inspiron 5494	1.16.0	01/12/2022
Inspiron 5510	2.6.1	01/11/2022
Inspiron 5593	1.19.0	01/13/2022
Inspiron 5594	1.16.0	01/12/2022
Inspiron 7490	1.11.0	01/13/2022
Inspiron 7510	1.4.0	01/07/2022
Inspiron 7610	1.4.0	01/07/2022
Latitude 3120	1.9.2	07/04/2022
Latitude 3190	1.21.1	07/06/2022
Latitude 3190 2-In-1	1.21.1	07/06/2022
Latitude 3320	1.8.2	12/09/2021
Latitude 5310	1.9.1	10/26/2022
Latitude 5310 2-in-1	1.9.1	10/26/2022
Latitude 5410	1.8.1	11/11/2021
Latitude 5411	1.8.1	11/09/2021
Latitude 5491	1.21.1	06/23/2022
Latitude 5510	1.8.1	11/11/2021
Latitude 5511	1.8.1	11/09/2021
Latitude 5591	1.21.1	06/23/2022
Latitude 7210 2-in-1	1.9.1	11/11/2021
Latitude 7310	1.9.1	11/10/2021
Latitude 7410	1.9.1	11/10/2021
Latitude 9410	1.9.1	11/10/2021

Latitude 9510	1.8.1	11/10/2021
OptiPlex 3060	1.20.0	06/15/2022
OptiPlex 3070	1.15.0	06/15/2022
OptiPlex 3080	2.11.0	05/11/2022
OptiPlex 3090	2.4.0	05/11/2022
OptiPlex 5060	1.20.0	06/15/2022
OptiPlex 5070	1.15.0	06/15/2022
OptiPlex 5080	1.11.0	05/11/2022
OptiPlex 5260 All-In-One	1.20.1	06/16/2022
OptiPlex 5270 All-in-One	1.15.1	06/15/2022
OptiPlex 7060	1.20.0	06/15/2022
OptiPlex 7070	1.15.0	06/15/2022
OptiPlex 7070 Ultra	1.13.2	06/08/2022
OptiPlex 7071	1.14.1	06/14/2022
OptiPlex 7080	1.11.0	05/10/2022
OptiPlex 7460 All-In-One	1.20.1	06/15/2022
OptiPlex 7470 All-in-One	1.15.1	06/15/2022
OptiPlex 7760 All-In-One	1.20.1	06/15/2022
OptiPlex 7770 All-in-One	1.15.1	06/15/2022
OptiPlex XE3	1.20.0	06/15/2022
Precision 3240 Compact	1.12.0	07/07/2022
Precision 3430 Tower	1.19.0	05/09/2022
Precision 3431 Tower	1.14.0	05/09/2022
Precision 3440	1.11.0	05/09/2022
Precision 3530	1.21.1	06/23/2022
Precision 3550	1.8.1	11/11/2021

Precision 3551	1.8.1	11/09/2021
Precision 3630 Tower	2.14.1	06/16/2022
Precision 3640 Tower	1.15.0	07/05/2022
Precision 3650 Tower	1.7.0	01/12/2022
Precision 3930 Rack	2.19.2	06/07/2022
Precision 7530	1.22.1	06/23/2022
Precision 7540	1.20.2	06/23/2022
Precision 7550	1.10.1	11/09/2021
Precision 7730	1.22.1	06/23/2022
Precision 7740	1.20.2	06/23/2022
Precision 7750	1.10.1	11/09/2021
Vostro 15 7580	1.21.0	05/10/2022
Vostro 3070	2.23.0	05/10/2022
Vostro 3401	1.11.0	01/13/2022
Vostro 3470	2.23.0	05/09/2022
Vostro 3480	1.19.0	05/10/2022
Vostro 3490	1.16.0	01/12/2022
Vostro 3501	1.11.0	01/13/2022
Vostro 3580	1.19.0	05/10/2022
Vostro 3583	1.19.0	05/10/2022
Vostro 3590	1.16.0	01/12/2022
Vostro 3670	2.23.0	05/10/2022
Vostro 3681	2.11.0	05/09/2022
Vostro 3881	2.11.0	05/09/2022
Vostro 3888	2.11.0	05/09/2022
Vostro 5090	1.14.0	05/10/2022

Vostro 5310	2.6.1	12/09/2021
Vostro 5410	2.6.1	01/11/2022
Vostro 5491	1.19.0	01/13/2022
Vostro 5510	2.6.1	01/11/2022
Vostro 5591	1.19.0	01/13/2022
Vostro 5880	1.11.0	05/10/2022
Vostro 7510	1.4.0	01/07/2022
Wyse 5070	1.17.0	05/10/2022
Wyse 5470	1.14.0	05/10/2022
Wyse 5470 All-In-One	1.15.0	05/10/2022
XPS 8940	2.6.0	05/11/2022

Revision History

Revision	Date	Description
1.0	2022/07/13	Initial Release

Related Information

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

Legal Disclaimer

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.

Affected Products

Inspiron, OptiPlex, G Series, G Series, Latitude, Vostro, Product Security Information

Article Properties

Article Number: 000201396

Article Type: Dell Security Advisory

Last Modified: 14 Jun 2023

Find answers to your questions from other Dell users

Visit Community

Support Services

Check if your device is covered by Support Services.

Check Support Status