Advisory Alert

Alert Number: AAA20230123 **Date:** January 23, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HP	**High**	Multiple vulnerabilities
Dell	**High**	Multiple vulnerabilities

Description

Affected Product	**HP**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-26316,CVE-2021-26398,CVE-2021-39298,CVE-2021-26402,CVE-2023-20530,CVE-2023-20531,CVE-2022-23813,CVE-2022-23814,CVE-2021-26328,CVE-2021-46768,CVE-2023-20522,CVE-2023-20525,CVE-2023-20527,CVE-2023-20528,CVE-2023-20532,CVE-2021-26353,CVE-2023-20523,CVE-2021-26404,CVE-2023-20529,CVE-2021-46791,CVE-2021-46779,CVE-2021-26409,CVE-2021-26407,CVE-2021-26403,CVE-2021-26396,CVE-2021-26343,CVE-2021-26355,CVE-2021-46767)
Description	HP has released a security update addressing multiple vulnerabilities in the BIOS firmware of HPE ProLiant Gen10 and Gen10 Plus servers with certain AMD EPYC processors. If exploited, these vulnerabilities can lead to denial of service, information disclosure, and arbitrary code execution. HP recommends to apply the necessary fixes at your earliest to avoid issues.
Affected Products	HPE ProLiant DL325 Gen10 Plus server - Prior to 2.60_08_11_2022 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to 2.60_08_11_2022 HPE ProLiant DL345 Gen10 Plus server - Prior to 2.60_08_11_2022 HPE ProLiant DL365 Gen10 Plus server - Prior to 2.60_08_11_2022 HPE ProLiant DL385 Gen10 Plus server - Prior to 2.60_08_11_2022 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to 2.60_08_11_2022 HPE ProLiant DL325 Gen10 Server - Prior to 2.60_08_11_2022 HPE ProLiant DL385 Gen10 Server - Prior to 2.60_08_11_2022 HPE ProLiant XL675d Gen10 Plus Server - Prior to 2.60_08_11_2022 HPE ProLiant XL645d Gen10 Plus Server - Prior to 2.60_08_11_2022 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to 2.60_08_11_2022
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04404en_us

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-35896,CVE-2022-35893,CVE-2022-36448,CVE-2022-35408,CVE-2022-36338,CVE-2022-35894,CVE-2022-35895)
Description	Dell has released a security update addressing Multiple vulnerabilities in Insyde UEFI. If exploited, these vulnerabilities can lead to information disclosure, memory corruption and arbitrary code execution. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell G15 5515 Dell G15 5525 Dell G5 5505 Inspiron 3505 Inspiron 3515 Inspiron 3525 Inspiron 3585 Inspiron 3785 Inspiron 5405 Inspiron 5415 Inspiron 5415 Inspiron 5425 Inspiron 5485 Inspiron 5485 2-in-1 Inspiron 5505 Inspiron 5515 Inspiron 5585 Inspiron 7405 2-in-1 Inspiron 7415 Inspiron 7425 Vostro 3405 Vostro 3425 Vostro 3515 Vostro 3525 Vostro 5415 Vostro 5515 Vostro 5625
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000207384/dsa-2023-007

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.