Advisory Alert

Alert Number: AAA20231129 **Date:** November 29, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Medium**	Sensitive Information Disclosure Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Sensitive Information Disclosure Vulnerabilities (CVE-2023-20594, CVE-2023-20597)
Description	HPE has released security updates addressing sensitive information disclosure vulnerabilities in their products. Potential security vulnerabilities have been identified in HPE Cray Servers and ProLiant DL/XL Servers using certain AMD EPYC processors. These vulnerabilities could be locally exploited to allow disclosure of sensitive information HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE Cray EX235n Server - Prior to BIOS 1.3.0 HPE Cray EX425 Compute Blade - Prior to BIOS 1.7.2 HPE ProLiant DL325 Gen10 Plus server - Prior to BIOS 2.64 HPE ProLiant DL385 Gen10 Plus server - Prior to BIOS 2.64 HPE ProLiant XL645d Gen10 Plus Server - Prior to BIOS 2.64 HPE ProLiant XL675d Gen10 Plus Server - Prior to BIOS 2.64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04540en_us

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28075, CVE-2023-32453)
Description	Dell has released security updates addressing an Improper Authentication and Time-of-check Time-of-use (TOCTOU) vulnerabilities in their products. **CVE-2023-28075** - A local authenticated malicious user with physical access to the system could potentially exploit this vulnerability by using a specifically timed DMA transaction during an SMI in order to gain arbitrary code execution on the system. **CVE-2023-32453** - Dell BIOS contains an improper authentication vulnerability. A malicious user with physical access to the system may potentially exploit this vulnerability in order to modify a security-critical UEFI variable without knowledge of the BIOS administrator Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000212817/dsa-2023-152-security-update-for-a-dell-client-bios-vulnerability https://www.dell.com/support/kbdoc/en-us/000215217/dsa-2023-190-security-update-for-a-dell-client-bios-vulnerability

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.