Advisory Alert

Alert Number: AAA20230516 **Date:** May 16, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	Medium	Out of Bounds Write Vulnerability
HP	Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	Medium
Affected Vulnerability	Out of Bounds Write Vulnerability (CVE-2023-25537)
Description	Dell has released a security update addressing an Out of Bounds Write Vulnerability exists in the Dell PowerEdge 14G Server BIOS. **CVE-2023-25537** – An out of bound vulnerability that exists in the Dell PowerEdge 14G server BIOS and Dell Precision BIOS, versions prior to 2.18.1. Using this vulnerability A local attacker with low privileges could expose some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PowerEdge R740, R740XD, R640, R940, R540, R440, T440, XR2, R740xD2, R840, R940xa, T640, C6420, FC640, M640, M640 (for PE VRTX), MX740c, MX840c, C4140, DSS 8440, XE2420, XE7420, XE7440 Versions prior to 2.18.1 Dell EMC Storage NX3240, NX3340 Versions prior to 2.18.1 Dell EMC XC Core 6420 System, XC640 System, XC740xd System, XC740xd2, XC940 System, XCXR2 Versions prior to 2.18.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability

Affected Product	**HP**
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-0060, CVE-2021-0147, CVE-2021-33068)
Description	HP has released a security update addressing multiple vulnerabilities that exists in certain HPE servers that using certain intel chipset firmware. These vulnerabilities could be locally exploited to allow privilege escalation or denial of service attacks HP recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE ProLiant m750 Server Blade - Prior to SPS_E3_05.01.04.400 HPE ProLiant MicroServer Gen10 Plus - Prior to SPS_E3_05.01.04.400 HPE ProLiant e910 Server Blade - Prior to SPS_E5_04.01.04.601 HPE ProLiant e910t Server Blade - Prior to SPS_E5_04.01.04.601 HPE ProLiant BL460c Gen10 Server Blade - Prior to SPS_E5_04.01.04.601 HPE Synergy 480 Gen10 Compute Module - Prior to SPS_E5_04.01.04.601 HPE Synergy 660 Gen10 Compute Module - Prior to SPS_E5_04.01.04.601 HPE ProLiant DL20 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DL120 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DL160 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DL180 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DL360 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DL380 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DL560 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DL580 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant ML30 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant ML110 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant ML350 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant XL230k Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant XL170r Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant XL190r Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant XL270d Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE ProLiant XL450 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE Apollo 4200 Gen10 Server - Prior to SPS_E5_04.01.04.601 HPE StoreEasy 1460 Storage - Prior to SPS_E5_04.01.04.601 HPE StoreEasy 1560 Storage - Prior to SPS_E5_04.01.04.601 HPE StoreEasy 1660 Expanded Storage - Prior to SPS_E5_04.01.04.601 HPE StoreEasy 1660 Storage - Prior to SPS_E5_04.01.04.601 HPE StoreEasy 1660 Performance Storage - Prior to SPS_E5_04.01.04.601 HPE StoreEasy 1860 Storage - Prior to SPS_E5_04.01.04.601 HPE StoreEasy 1860 Performance Storage - Prior to SPS_E5_04.01.04.601 HPE Storage Performance File Controller - Prior to SPS_E5_04.01.04.601 HPE Storage File Controller - Prior to SPS_E5_04.01.04.601 HPE ProLiant DX170r Gen10 server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DX190r Gen10 server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DX360 Gen10 server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DX380 Gen10 server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DX560 Gen10 server - Prior to SPS_E5_04.01.04.601 HPE ProLiant DX4200 Gen10 server - Prior to SPS_E5_04.01.04.601 HPE StoreOnce 3620 - Prior to SPS_E5_04.01.04.601 HPE StoreOnce 3640 - Prior to SPS_E5_04.01.04.601 HPE StoreOnce 5200 - Prior to SPS_E5_04.01.04.601 HPE StoreOnce 5250 - Prior to SPS_E5_04.01.04.601 HPE StoreOnce 5650 - Prior to SPS_E5_04.01.04.601
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04242en_us

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.