Advisory Alert

Alert Number: AAA20220621 **Date:** June 21, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
DELL	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	DELL
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-14584, CVE-2021-28210, CVE-2021-28211, CVE-2022-22558)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in the Dell PowerEdge products. **CVE-2019-14584, CVE-2021-28210, CVE-2021-28211** - Security vulnerabilities that exist in EDK2 could be exploited locally to allow authentication bypass and buffer overflow. **CVE-2022-22558** – Due to an Improper SMM communication buffer verification flaw that exists in Dell PowerEdge Server BIOS, a local high privileged attacker may potentially exploit this vulnerability leading to arbitrary writes or denial of service. Dell highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	PowerEdge DSS 8440 PowerEdge XR2 PowerEdge C4130 , C4140, C6320, C6420, C6520, C6525 PowerEdge FC430, FC630, FC640, FC830 PowerEdge M630, M630 (for PE VRTX), M640, PowerEdge M640 (for PE VRTX), M830, M830 (for PE VRTX) PowerEdge MX740c, MX750c, MX840c PowerEdge R230, R240, R250, R330, R340, PowerEdge R350, R430, R440, R450, R530 PowerEdge R540, R550, R630, R640, R6415 PowerEdge R650, R650xs, R6515, R6525, R730 PowerEdge R730xd, R740, R740xd, R740xd2, PowerEdge R7415, R7425, R750, R750xa, R750xs, PowerEdge R7515, R7525, R830, R840, R940, PowerEdge R940xa, T130, T140, T150, T330, PowerEdge T340, T350, T430, T440, T550, PowerEdge T630, T640 PowerEdge XE2420, XE7420, XE7440, XE8545, PowerEdge XR11, XR12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000198065/dsa-2022-088-dell-poweredge-server-bios-security-update-for-multiple-tianocore-edk2-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000197971/dsa-2022-015-dell-poweredge-improper-smm-communication-buffer-verification-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.