Advisory Alert

Alert Number: **AAA20230524** **Date:** **May 24, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Buffer underflow Vulnerability
Redhat	**High**	Use-after-free Vulnerability
Dell	**Medium**	Buffer underflow Vulnerability
VMware	**Medium**	Cross-site scripting Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Buffer underflow Vulnerability (CVE-2021-38578)
Description	Dell has released a security update addressing a Buffer underflow vulnerability that exists in Dell third party component Tianocore EDK2. **CVE-2021-38578** - Existing CommBuffer checks in SmmEntryPoint will not catch underflow when computing BufferSize. Dell highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PowerEdge T30 Versions prior to 1.11.0 PowerEdge T40 Versions prior to 1.11.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000214120/dsa-2023-183-dell-poweredge-t30-and-t40-mini-tower-security-update-for-an-tianocore-edk2-vulnerability

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2022-3564)
Description	Redhat has released security updates addressing a Use-after-free vulnerability that exists in their products. **CVE-2022-3564** - A use-after-free flaw was found in the Linux kernel's L2CAP bluetooth functionality in how a user triggers a race condition by two malicious flows in the L2CAP bluetooth packets. This flaw allows a local or bluetooth connection user to crash the system or potentially escalate privileges. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server - AUS 7.7 x86_64 Red Hat Enterprise Linux Server - TUS 7.7 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.7 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:3278 https://access.redhat.com/errata/RHSA-2023:3277

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Buffer underflow Vulnerability (CVE-2021-38578)
Description	Dell has released a security update addressing a Buffer underflow vulnerability that exists in Dell third party component Tianocore EDK2. **CVE-2021-38578** - Existing CommBuffer checks in SmmEntryPoint will not catch underflow when computing BufferSize. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell EMC NX440 Versions prior to 2.13.1 Dell EMC Storage NX3240 Versions prior to 2.18.1 Dell EMC Storage NX3340 Versions prior to 2.18.1 Dell EMC XC Core 6420 System Versions prior to 2.18.1 Dell EMC XC Core XC640 System Versions prior to 2.18.1 Dell EMC XC Core XC740xd System Versions prior to 2.18.1 Dell EMC XC Core XC940 System Versions prior to 2.18.1 Dell EMC XC Core XCXR2 Versions prior to 2.18.1 Dell Storage NX3230 Versions prior to 2.17.0 Dell Storage NX3330 Versions prior to 2.17.0 Dell Storage NX430 Versions prior to 2.17.0 Dell XC430 Hyper-converged Appliance Versions prior to 2.17.0 Dell XC630 Hyper-converged Appliance Versions prior to 2.17.0 Dell XC6320 Hyper-converged Appliance Versions prior to 2.17.0 DSS 8440 Versions prior to 2.18.1 PowerEdge C4130 Versions prior to 2.17.0 PowerEdge C4140 Versions prior to 2.18.1 PowerEdge C6320 Versions prior to 2.17.0 PowerEdge C6420 Versions prior to 2.18.1 PowerEdge C6520 Versions prior to 1.10.2 PowerEdge C6525 Versions prior to 2.11.3 PowerEdge C6620 Versions prior to 1.2.1 PowerEdge FC640 Versions prior to 2.18.1 PowerEdge M640 Versions prior to 2.18.1 PowerEdge M640 (for PE VRTX) Versions prior to 2.18.1 PowerEdge MX740C Versions prior to 2.18.1 PowerEdge MX750c Versions prior to 1.10.2 PowerEdge MX760c Versions prior to 1.2.1 PowerEdge MX840C Versions prior to 2.18.1 PowerEdge R230 Versions prior to 2.17.0 PowerEdge R240 Versions prior to 2.13.1 PowerEdge R250 Versions prior to 1.6.3 PowerEdge R330 Versions prior to 2.17.0 PowerEdge R340 Versions prior to 2.13.1 PowerEdge R350 Versions prior to 1.6.3 PowerEdge R440 Versions prior to 2.18.1 PowerEdge R450 Versions prior to 1.10.2 PowerEdge R540 Versions prior to 2.18.1 PowerEdge R550 Versions prior to 1.10.2 PowerEdge R630 Versions prior to 2.17.0 PowerEdge R640 Versions prior to 2.18.1 PowerEdge R6415 Versions prior to 1.20.0 PowerEdge R650 Versions prior to 1.10.2 PowerEdge R650XS Versions prior to 1.10.2 PowerEdge R6515 Versions prior to 2.11.4 PowerEdge R6525 Versions prior to 2.11.3 PowerEdge R660 Versions prior to 1.2.1 PowerEdge R6615 Versions prior to 1.3.11 PowerEdge R6625 Versions prior to 1.3.11 PowerEdge R730 Versions prior to 2.17.0 PowerEdge R730xd Versions prior to 2.17.0 PowerEdge R740 Versions prior to 2.18.1 PowerEdge R740XD Versions prior to 2.18.1 PowerEdge R740XD2 Versions prior to 2.18.1 PowerEdge R7415 Versions prior to 1.20.0 PowerEdge R7425 Versions prior to 1.20.0 PowerEdge R750 Versions prior to 1.10.2 PowerEdge R750XA Versions prior to 1.10.2 PowerEdge R750XS Versions prior to 1.10.2 PowerEdge R7515 Versions prior to 2.11.4 PowerEdge R7525 Versions prior to 2.11.3 PowerEdge R760 Versions prior to 1.2.1 PowerEdge R7615 Versions prior to 1.3.11 PowerEdge R7625 Versions prior to 1.3.11 PowerEdge R830 Versions prior to 1.17.0 PowerEdge R840 Versions prior to 2.18.1 PowerEdge R930 Versions prior to 2.12.0 PowerEdge R940 Versions prior to 2.18.1 PowerEdge R940XA Versions prior to 2.18.1 PowerEdge T130 Versions prior to 2.17.0 PowerEdge T140 Versions prior to 2.13.1 PowerEdge T150 Versions prior to 1.6.3 PowerEdge T330 Versions prior to 2.17.0 PowerEdge T340 Versions prior to 2.13.1 PowerEdge T350 Versions prior to 1.6.3 PowerEdge T440 Versions prior to 2.18.1 PowerEdge T550 Versions prior to 1.10.2 PowerEdge T630 Versions prior to 2.17.0 PowerEdge T640 Versions prior to 2.18.1 PowerEdge XE8545 Versions prior to 2.11.2 PowerEdge XR11 Versions prior to 1.10.2 PowerEdge XR12 Versions prior to 1.10.2 PowerEdge XR2 Versions prior to 2.18.1 PowerEdge XR4510c Versions prior to 1.10.4 PowerEdge XR4520c Versions prior to 1.10.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000214125/dsa-2023-097-security-update-for-dell-poweredge-server-for-tianocore-edk2-vulnerability

Affected Product	**VMware**
Severity	**Medium**
Affected Vulnerability	Cross-site scripting vulnerability (CVE-2023-20868)
Description	VMware has released a security update for a cross-site scripting vulnerability that exists in their products. **CVE-2023-20868** - NSX-T contains a reflected cross-site scripting vulnerability due to a lack of input validation. A remote attacker can inject HTML or JavaScript to redirect to malicious pages. VMware recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cloud Foundation (NSX-T) 4.5.x NSX-T 3.2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0010.html

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.