



Advisory Alert

Alert Number: AAA20220912

Date: September 12, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
DELL	High	Cross Site Scripting Vulnerability
HP	High	Multiple Vulnerabilities

Description

Affected Product	DELL
Severity	High
Affected Vulnerability	Cross Site Scripting Vulnerability (CVE-2021-46827)
Description	<p>Dell has released a security update addressing a Cross Site Scripting Vulnerability that exists in the third party component named as Oxygen XML WebHelp that is used in multiple DELL products. This vulnerability allows an attacker to execute JavaScript by convincing a user to type specific text in the WebHelp output search field.</p> <p>Dell highly recommends to apply necessary security fixes at earliest to avoid issues.</p>
Affected Products	Unisphere for PowerMax - Versions before 9.2.3.15 Unisphere for PowerMax Virtual Appliance - Versions before 9.2.3.15 Solutions Enabler Virtual Appliance - Versions before 9.2.3.4 eVASA Provider Virtual Appliance - Versions before 9.2.3.7 VASA Provider Standalone - Versions before 9.2.3.15 PowerMaxOS – version 5978.711.711
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000203182/dsa-2022-119-dell-unisphere-for-powermax-dell-unisphere-for-powermax-vapp-dell-solutions-enabler-vapp-dell-unisphere-360-dell-vasa-provider-vapp-and-dell-powermax-emb-mgmt-security-update-for-an-oxygen-xml-webhelp-vulnerability

Affected Product	HP
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-0190, CVE-2021-0155, CVE-2021-0189, CVE-2021-0154)
Description	<p>HP has released a security update addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities could cause information disclosure and privilege escalation.</p> <p>HP highly recommends to apply necessary security fixes at earliest to avoid issues</p>
Affected Products	HPE Integrity MC990 X Server - Prior to 5.2.16 BIOS in product bundle 2022.06 HPE HPE Superdome Flex 280 Server - Prior to 1.35.12 HPE Superdome Flex 280 Server - Prior to 1.35.12 SGI UV 300 - Prior to 5.2.16 BIOS in product bundle 2022.06 SGI UV 3000 - Prior to 4.0.9 BIOS in product bundle 2022.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04314en_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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted | Public

Report incident to incident@fincsirt.lk

TLP: WHITE