TLP: WHITE

Advisory Alert

Alert Number: **AAA20240628** **Date:** **June 28, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
WatchGuard	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple vulnerabilities
VMware Broadcom	**Medium**	Injection Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23820, CVE-2021-46774, CVE-2023-20533, CVE-2023-20519, CVE-2023-20566, CVE-2023-20521, CVE-2021-46766, CVE-2022-23830, CVE-2023-20526, CVE-2021-26345)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, Code Execution, Denial of Service (DoS), Elevated Privileges and Buffer Overflow. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL325 Gen10 Plus server - Prior to 2.84 (HFP 23.9) HPE ProLiant DL385 Gen10 Plus server - Prior to 2.84 (HFP 23.9) HPE ProLiant XL645d Gen10 Plus Server - Prior to 2.84 (HFP 23.9) HPE ProLiant XL675d Gen10 Plus Server - Prior to 2.84 (HFP 23.9) HPE Cray EX235a Accelerator Blade - Prior to 1.8.0 (HFP 24.3.1) HPE Cray EX235n Server - Prior to 1.3.1 (HFP 23.9) HPE Cray EX425 Compute Blade - Prior to 1.7.2 (HFP 23.9) - Gen 2, and Gen 3 EPYC Processors. HPE Cray EX4252 Compute Blade - Prior to 1.4.0 (HFP 23.8)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04657en_us&docLocale=en_US

Affected Product	**WatchGuard**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-4944, CVE-2024-5974)
Description	WatchGuard has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-4944 -** A local privilege escalation vulnerability in the WatchGuard Mobile VPN with SSL client on Windows enables a local user to execute arbitrary commands with elevated privileged. **CVE-2024-5974 -** A buffer overflow in WatchGuard Fireware OS could may allow an authenticated remote attacker with privileged management access to execute arbitrary code with system privileges on the firewall. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WatchGuard Mobile VPN with SSL for Windows up to and including version 12.10 Fireware OS 11.9.4 through 12.5.12_Update1 and Fireware 12.6 through 12.10.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00010 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00011

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerMaxOS 10.1.0.2 - PowerMax OS - Version prior to 10.1.0.3 Patch 10410 Dell PowerMax EEM - Embedded Management - Version prior to 10.1.0.3 Patch 10410 Dell PowerMax EEM - Embedded Management - Version prior to 5978.714.714 patch 10408 PowerMaxOS 5978.714.714 - PowerMax OS - Version prior to 5978.714.714 patch 10408 Solutions Enabler Host Installation - Versions prior to 10.1.0.3 Unisphere for PowerMax - Host Installation - Versions prior to 10.1.0.6 Unisphere for PowerMax Virtual Appliance - Virtual Appliance Versions prior to 9.2.4.10 Unisphere 360 - Host Installation - Versions prior to 9.2.4.18 Solutions Enabler Virtual Appliance Virtual Appliance - Versions prior to 9.2.4.6 version 84 Q2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226453/dsa-2024-275-dell-powermaxos-5978-dell-powermax-os-10-1-0-2-dell-unisphere-360-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-solutions-enabler-virtual-appliance-and-dell-powermax-eem-security-update-for-multiple-vul

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2024-34064, CVE-2024-3651, CVE-2024-26130, CVE-2023-45288, CVE-2024-25031, CVE-2024-38322, CVE-2024-33883, CVE-2022-38383)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to Cross-site Scripting, Denial of Service NULL Pointer Dereference, Information Exposure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect Plus File Systems Agent Version - 10.1.6 - 10.1.16.1 IBM Storage Defender - Resiliency Service - Version 2.0.0-2.0.4 IBM Cloud Pak for Security - Version 1.10.0.0 - 1.10.11.0 QRadar Suite Software - Version 1.10.12.0 - 1.10.21.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7158820 • https://www.ibm.com/support/pages/node/7158446 • https://www.ibm.com/support/pages/node/7158986

Affected Product	**VMware Broadcom**
Severity	**Medium**
Affected Vulnerability	Injection Vulnerability (CVE-2024-22260)
Description	Broadcom has released security updates addressing an Injection Vulnerability that exists in VMware Workspace ONE UEM. A malicious actor with network access to the Workspace One UEM may be able to perform an attack resulting in an information exposure. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Workspace One UEM - Version 23.10.x VMware Workspace One UEM - Version 23.6.x VMware Workspace One UEM - Version 22.12.x VMware Workspace ONE UEM - Version 23.2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/OMSA-2024-0001.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.