Advisory Alert

Alert Number: AAA20241007 **Date:** October 7, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Remote Buffer Overflow Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Remote Buffer Overflow Vulnerability (CVE-2021-38578)
Description	HPE has released security updates addressing a Remote Buffer Overflow Vulnerability that exists in HPE SimpliVity Servers. **CVE-2021-38578** - Existing CommBuffer checks in SmmEntryPoint will not catch underflow when computing BufferSize. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• HPE SimpliVity 325 Gen 11 - Prior to HPE SimpliVity Gen11 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 380 Gen11 - Prior to HPE SimpliVity Gen11 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 170r Gen10 Server - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 190r Gen10 Server - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 2600 Gen10 - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 325 Gen10 - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 325 Gen10 Plus - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 380 Gen10 - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 380 Gen10 G - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 380 Gen10 H - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930 • HPE SimpliVity 380 Gen10 Plus - Prior to HPE SimpliVity Gen10 Support Pack (SVTSP) v2024_0930
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04716en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6345, CVE-2024-45099, CVE-2024-45642, CVE-2024-26671)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar and IBM Storage Copy Data Management. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Cross-site Scripting, Sensitive Information Disclosure and Arbitrary Code Execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR version 3.12 IBM Storage Copy Data Management versions 2.2.0.0 - 2.2.24.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7172419 • https://www.ibm.com/support/pages/node/7172212 • https://www.ibm.com/support/pages/node/7172211

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-20434)
Description	Cisco has released security updates addressing a Denial of Service Vulnerability that exists in Cisco Catalyst 9000 Series Switches. **CVE-2024-20434** - Due to improper handling of frames with VLAN tag information, an attacker could send crafted frames to an affected device. A successful exploit could allow the attacker to render the control plane of the affected device unresponsive. The device would not be accessible through the console or CLI, and it would not respond to ping requests, SNMP requests, or requests from other control plane protocols. Traffic that is traversing the device through the data plane is not affected. A reload of the device is required to restore control plane services. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following products running on a vulnerable release of Cisco IOS XE Software (Use Cisco Software Checker to identify vulnerable versions) • Catalyst 9300LM Series Switches • Catalyst 9300X Series Switches • Catalyst 9400X Supervisor Engines • Catalyst 9500 High Performance Series Switches • Catalyst 9600 Series Switches
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vlan-dos-27Pur5RT

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.