Advisory Alert

Alert Number: AAA20240408 **Date:** April 8, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Medium**	Remote Authentication Bypass Vulnerability
Dell	**Medium**	Denial of Service Vulnerability
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Remote Authentication Bypass Vulnerability (CVE-2023-48795)
Description	HPE has released security updates addressing a Remote Authentication Bypass Vulnerability that exists in HPE SimpliVity Servers. This vulnerability could be locally exploited to allow remote attackers to bypass integrity checks. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SimpliVity Omnistack for HPE - Version 4.2.0 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04596en_us

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2011-1473)
Description	Dell has released security updates addressing a Denial of Service Vulnerability that exists in Dell NetWorker Management Console. **CVE-2011-1473** - OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetWorker Management Console Versions 19.10 NetWorker Management Console Versions prior to 19.8.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223843/dsa-2023-165-security-update-for-dell-networker-openssl-vulnerabilities

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28784, CVE-2022-32751, CVE-2024-27088, CVE-2024-28849)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Cross-Site Scripting, Sensitive Server Information Disclosure and Denial of Service. IBM recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP7 IF06 IBM Security Verify Directory versions 10.0.0.0 - 10.0.0.1 IBM Security Directory Server versions 6.4.0.0 - 6.4.0.27 IBM Storage Defender - Resiliency Service versions 2.0.0 - 2.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145260 • https://www.ibm.com/support/pages/node/7147552 • https://www.ibm.com/support/pages/node/7145945

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.