Advisory Alert

Alert Number: AAA20241101 **Date:** November 1, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**High**	Denial of Service Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-41996)
Description	F5 has released security updates addressing a Denial of Service Vulnerability that exist in their products. **CVE-2024-41996 -** Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE and validate the order of the public key. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5 BIG-IP Versions - 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000148343

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-37891, CVE-2024-34062, CVE-2024-39689, CVE-2024-5569, CVE-2024-3651, CVE-2024-35195)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Sensitive Information Disclosure, Execute Arbitrary Code. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar App SDK Versions - 1.0.0 - 2.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7174420

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7088-1

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-50782, CVE-2023-52425, CVE-2024-39586, CVE-2023-22025, CVE-2023-22067, CVE-2023-22081, CVE-2024-47475)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell 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	Dell EMC AppSync Versions 4.3.0.0 through 4.6.0.0 Dell OpenManage Server Administrator Managed Node • for Windows versions prior to 11.1.0.0 • for (Linux Consolidated) versions prior to 11.1.0.0 • for RHEL 8.x versions prior to 11.1.0.0 • for RHEL 9.x versions prior to 11.1.0.0 • for SLES 15 versions prior to 11.1.0.0 Dell Systems Management Tools and Documentation DVD ISO versions prior to 11.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000234216/dsa-2024-420-security-update-for-dell-emc-appsync-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000228093/dsa-2024-150-security-update-for-dell-openmanage-server-administrator-omsa-network-access-vulnerability • https://www.dell.com/support/kbdoc/en-us/000242681/dsa-2024-417-security-update-for-dell-powerscale-onefs-for-security-vulnerability

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.