Advisory Alert

Alert Number: **AAA20241112** **Date:** **November 12, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Synology	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Synology	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
F5	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities
Fortiguard	**Medium**	RADIUS Protocol Vulnerability

Description

Affected Product	**Synology**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Synology has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities may lead to arbitrary code execution, writing of specific files, hijacking of admin sessions. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Synology DSM 7.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_24_20

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-16931, CVE-2017-7376, CVE-2016-4658, CVE-2015-8710, CVE-2016-4448, CVE-2017-7375, CVE-2021-3518, CVE-2016-5131, CVE-2017-15412, CVE-2017-5130, CVE-2021-3517, CVE-2016-1762, CVE-2016-1840, CVE-2022-40304, CVE-2016-1834, CVE-2015-6838, CVE-2019-19956, CVE-2017-16932, CVE-2022-40303, CVE-2016-3627, CVE-2013-1969, CVE-2022-23308, CVE-2016-4447, CVE-2015-6837, CVE-2024-25062, CVE-2016-4483, CVE-2018-14404, CVE-2015-8806, CVE-2015-5312, CVE-2016-4449, CVE-2013-0339, CVE-2012-5134, CVE-2012-2871, CVE-2016-9596, CVE-2023-28484, CVE-2023-45322, CVE-2023-29469, CVE-2022-29824, CVE-2016-2073, CVE-2017-18258, CVE-2021-3541, CVE-2016-9598, CVE-2015-8241, CVE-2021-3537, CVE-2015-8242, CVE-2016-1837, CVE-2016-1838, CVE-2016-9318, CVE-2016-1833, CVE-2016-1836, CVE-2016-1839, CVE-2015-7500, CVE-2015-8317, CVE-2013-2877, CVE-2015-7497, CVE-2015-7499, CVE-2014-3660, CVE-2015-7498, CVE-2013-0338)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in third party products that in turn affect 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 NetWorker Server Versions 19.11 through 19.11.0.1 Dell NetWorker Server Versions 19.10 through 19.10.0.5 Dell NetWorker Server Versions 19.9 through 19.9.0.7 Dell NetWorker Server Versions 19.8 through 19.8.0.4 Dell NetWorker Server Versions prior to 19.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000247018/dsa-2024-251-security-update-for-dell-networker-for-libxml2-2-9-0-vulnerabilities

Affected Product	**Synology**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Synology has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may allow remote attackers to hijack web sessions and inject SQL commands via a susceptible version of Synology Drive Server. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Synology Drive Server for DSM 7.1, 7.2.1 and 7.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_24_21

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-48837, CVE-2024-48838, CVE-2024-49557, CVE-2024-49558, CVE-2024-49560)
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	Dell Networking OS10 10.5.6.x, 10.5.5.x and 10.5.4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000247217/dsa-2024-425-security-update-for-dell-networking-os10-vulnerabilities

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5981, CVE-2024-0553, CVE-2024-25062, CVE-2023-52881)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-5981** - A vulnerability was found that the response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding. **CVE-2024-0553** - A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. **CVE-2024-25062** - An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free. **CVE-2023-52881** - This vulnerability allows an attacker to brute force the server-chosen send window by acknowledging data that was never sent, called "ghost ACKs." There are side channels that also allow the attacker to leak the otherwise secret server-chosen initial sequence number (ISN). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10, 8.0.0 - 8.3.0 BIG-IP Next (all modules) 20.0.1 - 20.0.2 BIG-IP Next Central Manager 20.0.1 - 20.0.2 BIG-IP Next CNF 1.1.0 - 1.3.1 BIG-IP Next SPK 1.5.0 - 1.9.2 BIG-IQ Centralized Management 8.2.0 - 8.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000138649 • https://my.f5.com/manage/s/article/K000141357 • https://my.f5.com/manage/s/article/K000148479

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21698, CVE-2024-45086, CVE-2024-45087)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-21698** - Prometheus Go client library (client_golang) is vulnerable to a denial of service, caused by a flaw when handling requests with non-standard HTTP methods. By sending specially-crafted HTTP requests, a remote attacker could exploit this vulnerability to cause a memory exhaustion. **CVE-2024-45086** - IBM WebSphere Application Server is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources. **CVE-2024-45087** - IBM WebSphere Application Server is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Data Protect 1.0.0 - 2.0.6 IBM WebSphere Application Server 9.0 and 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7173172 • https://www.ibm.com/support/pages/node/7174745 • https://www.ibm.com/support/pages/node/7175393

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-43908,CVE-2024-43854,CVE-2024-42296,CVE-2024-43914,CVE-2024-46798,CVE-2024-46746,CVE-2024-42290,CVE-2024-46685,CVE-2024-44935,CVE-2024-41098,CVE-2024-45018,CVE-2022-48666,CVE-2024-43890,CVE-2024-46689,CVE-2024-42289,CVE-2024-46719,CVE-2024-46722,CVE-2024-38577,CVE-2024-46745,CVE-2024-47668,CVE-2024-42306,CVE-2024-42299,CVE-2024-43856,CVE-2024-44948,CVE-2024-46743,CVE-2024-41068,CVE-2024-43834,CVE-2024-44958,CVE-2024-45028,CVE-2024-42288,CVE-2024-41091,CVE-2024-43884,CVE-2024-41011,CVE-2024-39472,CVE-2024-46817,CVE-2024-43841,CVE-2024-44995,CVE-2024-46761,CVE-2024-45026,CVE-2024-47660,CVE-2024-42114,CVE-2024-43883,CVE-2024-44952,CVE-2024-46723,CVE-2024-46677,CVE-2024-43817,CVE-2024-42281,CVE-2024-45009,CVE-2024-41012,CVE-2024-41070,CVE-2024-38611,CVE-2024-46759,CVE-2024-41073,CVE-2024-46702,CVE-2024-44969,CVE-2024-46814,CVE-2024-41072,CVE-2024-42309,CVE-2024-43853,CVE-2024-46747,CVE-2024-45006,CVE-2024-42267,CVE-2024-44986,CVE-2024-43830,CVE-2024-41064,CVE-2024-42259,CVE-2024-42311,CVE-2024-44934,CVE-2024-44990,CVE-2024-46807,CVE-2024-43835,CVE-2024-42246,CVE-2024-46763,CVE-2024-41020,CVE-2024-41071,CVE-2024-44974,CVE-2024-43858,CVE-2024-42269,CVE-2024-410)
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 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7100-1

Affected Product	**Fortiguard**
Severity	**Medium**
Affected Vulnerability	RADIUS Protocol Vulnerability (CVE-2024-3596)
Description	Fortiguard has released security updates addressing RADIUS Protocol Vulnerability that exists in their products. **CVE-2024-3596** - A fundamental design flaw within the RADIUS protocol has been proven to be exploitable, compromising the integrity in the RADIUS Access-Request process. The attack allows a malicious user to modify packets in a way that would be indistinguishable to a RADIUS client or server. To be successful, the attacker must have the ability to inject themselves between the client and server. Fortiguard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiProxy 7.4.0 through 7.4.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-255

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.