Advisory Alert

Alert Number: AAA20240927 **Date:** September 27, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PHP	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Security Update
Red Hat	**High**	Out-Of-Bounds Buffer overflow Vulnerability
Dell	**High**	Multiple Vulnerabilities
Juniper	**High**	Blast-RADIUS Vulnerability
NetApp	**High**, Medium	Multiple Vulnerabilities
Synology	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**PHP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-4577, CVE-2024-8926, CVE-2024-8927, CVE-2024-9026, CVE-2024-8925)
Description	PHP has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Parameter injection, Configuration bypass. PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP 8.3.x versions prior to 8.3.12 PHP 8.2.x versions prior to 8.2.24 PHP 8.1.x versions prior to 8.1.30
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.php.net/ChangeLog-8.php#PHP_8_3 • https://www.php.net/ChangeLog-8.php#PHP_8_2 • https://www.php.net/ChangeLog-8.php#PHP_8_1

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2024-45409)
Description	NetApp has released a security update addressing a vulnerability that exists in the Ruby-SAML third-party product which in turn affects NetApp products. **CVE-2024-45409** - Multiple NetApp products incorporate Ruby-SAML. Certain versions of Ruby-SAML are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240926-0008/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Out-Of-Bounds Buffer overflow Vulnerability (CVE-2024-41071)
Description	Red Hat has released security updates addressing an Out-Of-Bounds Buffer overflow Vulnerability that exists in their products. The vulnerability is found in the Linux kernel's mac80211 subsystem when scanning for SSIDs. Address calculation using out-of-bounds array indexing could result in an attacker crafting an exploit, resulting in the complete compromise of a system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 i386 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension (for IBM z Systems) 6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:7227

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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000229094/dsa-2024-408-dell-powerstore-family-security-update-for-multiple-vulnerabilitiesV • https://www.dell.com/support/kbdoc/en-us/000229085/dsa-2024-375-dell-powermaxos-5978-714-714-dell-powermax-os-10-1-0-5-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-mult • https://www.dell.com/support/kbdoc/en-us/000228976/dsa-2024-274-security-update-for-dell-networking-os10-vulnerabilities

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Blast-RADIUS Vulnerability (CVE-2024-3596)
Description	Juniper has released security updates addressing the Blast-RADIUS Vulnerability that exists in their products. **CVE-2024-3596** - RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. Juniper Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Below implementations of Infrastructure devices (RADIUS client), RADIUS servers and protocols. • Non-EAP based authentications such as PAP / CHAP / MS-CHAP • Communicating over UDP in the clear • Without Message-Authenticator in requests and response
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/Mist-RADIUS-Protocol-Vulnerability-Blast-RADIUS-CVE-2024-3596?language=en_US

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45287, CVE-2024-36902)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-45287** - ONTAP 9 incorporates FreeBSD. All supported versions of FreeBSD are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2024-36902** - Multiple NetApp products incorporate Linux kernel. Certain versions of Linux kernel are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 (formerly Clustered Data ONTAP) E-Series SANtricity OS Controller Software 11.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20240926-0002/ • https://security.netapp.com/advisory/ntap-20240926-0010/

Affected Product	**Synology**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52946, CVE-2022-49037, CVE-2022-49038, CVE-2022-49039, CVE-2022-49040, CVE-2022-49041, CVE-2023-52950, CVE-2023-52947, CVE-2023-52948, CVE-2023-52949)
Description	Synology has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to buffer overflow, sensitive information disclosure, privilege escalation. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Synology Drive Client prior to 3.5.0-16084 version Synology Active Backup for Business Agent prior to 2.7.0-3221 version
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.synology.com/en-global/security/advisory/Synology_SA_24_10 • https://www.synology.com/en-global/security/advisory/Synology_SA_24_11

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7039-1 • https://ubuntu.com/security/notices/USN-7021-3

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.