Advisory Alert

Alert Number: **AAA20240307** **Date:** **March 7, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	Access Bypass Vulnerability
NETGEAR	**High**	Post-Authentication Stack Overflow Vulnerability
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Kernel vulnerabilities
Red Hat	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has released a security patch update addressing an Access Bypass vulnerability in Drupal Registration role Module. The module has a logic error when handling sites that upgraded code and did not run the Drupal update process (e.g. update.php). Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Drupal Registration role module version 2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-015

Affected Product	**NETGEAR**
Severity	**High**
Affected Vulnerability	Post-Authentication Stack Overflow Vulnerability (CVE-2023-48725)
Description	Netgear has released a security update addressing a post-authentication stack overflow security vulnerability. This vulnerability requires an attacker to have your WiFi password or an Ethernet connection to a device on your network to be exploited. Netgear recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Netgear Routers • RAX28 -firmware versions before 1.0.13.102_HOTFIX • RAX29 -firmware versions before 1.0.13.102_HOTFIX • RAX30 -firmware versions before 1.0.13.102_HOTFIX
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000066037/Security-Advisory-for-Post-Authentication-Stack-Overflow-on-the-RAX30-PSV-2023-0160?article=000066037

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20345,CVE-2024-20346, CVE-2024-20292, CVE-2024-20301, CVE-2024-20337, CVE-2024-20338)
Description	Cisco has released security updates addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Path traversal, Cross-Site Scripting, Information Disclosure, Authentication Bypass, and Privilege Escalation. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco AppDynamics Controller Earlier than 23.4.0 Cisco Duo Authentication for Windows Logon and RDP 4.0.0 through 4.0.7, 4.1.0 through 4.1.3, 4.2.0 through 4.2.2 All versions of Cisco Small Business 100, 300, and 500 Series Wireless APs and firmware Cisco Secure Client 4.10.04065 and later, 5.0, 5.1 Cisco Secure Client for Linux Earlier than 5.1.2.42
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-traversal-m7N8mZpF https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-xss-3JwqSMNT https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-infodisc-rLCEqm6T https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-win-bypass-pn42KKBm https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-client-crlf-W43V4G7#vp https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-privesc-sYxQO6ds

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Kernel vulnerabilities (CVE-2023-46343, CVE-2023-51782, CVE-2023-6121, CVE-2023-51779, CVE-2024-0607, CVE-2023-6560, CVE-2024-25744, CVE-2023-22995, CVE-2023-51780, CVE-2021-44879, CVE-2024-0340, CVE-2023-4244)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in their Linux kernel. These vulnerabilities cause Denial of service, Arbitrary code execute, Sensitive information disclosure. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 20.04 Ubuntu 18.04 Ubuntu 23.10 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6680-1 https://ubuntu.com/security/notices/USN-6681-1

Affected Product	**Red Hat**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-43975, CVE-2022-1055, CVE-2022-2938, CVE-2022-27950, CVE-2022-41674, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722, CVE-2022-45869, CVE-2023-0597, CVE-2023-6606, CVE-2023-7192, CVE-2023-51043, CVE-2024-0565, CVE-2023-48795, CVE-2023-4043, CVE-2023-4759, CVE-2023-35887)
Description	Red Hat has released security updates addressing multiple vulnerabilities. These vulnerabilities could be exploited to cause Out of bounds write, Denial of service, User after free condition, Remote code execution. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 9 x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1188 https://access.redhat.com/errata/RHSA-2024:1197 https://access.redhat.com/errata/RHSA-2024:1196 https://access.redhat.com/errata/RHSA-2024:1194 https://access.redhat.com/errata/RHSA-2024:1193 https://access.redhat.com/errata/RHSA-2024:1192

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.