Advisory Alert

Alert Number: **AAA20240222** **Date:** **February 22, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Netgear	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Low**	Access Bypass Vulnerability

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6546, CVE-2024-0822)
Description	Red Hat has released security updates addressing multiple vulnerabilities. **CVE-2023-6546** - A race condition was found in the GSM 0710 tty multiplexor in the Linux kernel. This issue occurs when two threads execute the GSMIOC_SETCONF ioctl on the same tty file descriptor with the gsm line discipline enabled, and can lead to a use-after-free problem on a struct gsm_dlci while restarting the gsm mux. **CVE-2024-0822** - An authentication bypass vulnerability was found in overt-engine. This flaw allows the creation of users in the system without authentication due to a flaw in the CreateUserSession command. 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 Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux Server - TUS 8.6 x86_64 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 Virtualization Manager 4.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0937 https://access.redhat.com/errata/RHSA-2024:0934

Affected Product	**Netgear**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Netgear has released security updates addressing multiple vulnerabilities that exist Netgear routers and extenders. Exploitation of these vulnerabilities could lead to Command injection and more flaws. Netgear recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	EX3700 fixed in firmware version 1.0.0.98 EX3800 fixed in firmware version 1.0.0.98 EX6120 fixed in firmware version 1.0.0.70 XR1000 fixed in firmware version 1.0.0.72 R7000 fixed in firmware version 1.0.11.216
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000066030/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Extenders-PSV-2023-0150-PSV-2023-0151 https://kb.netgear.com/000066029/Security-Advisory-for-Post-Authentication-Command-Injection-on-the-XR1000-PSV-2023-0152?article=000066029 https://kb.netgear.com/000066028/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-Extenders-PSV-2023-0153?article=000066028 https://kb.netgear.com/000066027/Security-Advisory-for-Post-Authentication-Command-Injection-on-the-R7000-PSV-2023-0154?article=000066027

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20325, CVE-2020-3259)
Description	Cisco has released security updates addressing multiple vulnerabilities. **CVE-2024-20325** - An Insufficient Access Control Vulnerability exists in the Live Data server of Cisco Unified Intelligence Center caused due to insufficient access control implementations on cluster configuration CLI requests. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device. **CVE-2020-3259** - An Information Disclosure Vulnerability exists in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software causes due to a buffer tracking issue when the software parses invalid URLs that are requested from the web services interface. A successful exploit could allow the attacker to retrieve memory contents, which could lead to the disclosure of confidential information. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Unified Intelligence Center Release 12.5(1) and earlier, 12.5(2), 12.6(1), 12.6(2) Cisco ASA Software Release Earlier than 9.51, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.12, 9.13, 9.14 Cisco FTD Software Release Earlier than 6.2.31, 6.2.3, 6.3.0, 6.4.0, 6.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-access-control-jJsZQMjj https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51781, CVE-2024-0646, CVE-2024-0565, CVE-2023-6915, CVE-2023-7192, CVE-2023-51780, CVE-2023-51782)
Description	Ubuntu has released security updates addressing multiple vulnerabilities. An attacker exploit these vulnerabilities to cause Denial of service (system crash/ memory Exhaustion) or possibly execute Arbitrary code and 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 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6648-1 https://ubuntu.com/security/notices/USN-6647-1

Affected Product	**F5**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-28733, CVE-2023-46218)
Description	F5 has released security updates addressing multiple vulnerabilities. **CVE-2022-28733** - This flaw allows an attacker to craft a malicious packet, triggering an integer underflow in grub code. Consequently, the memory allocation for handling the packet data may be smaller than the size needed. This issue causes an out-of-bands write during packet handling, compromising data integrity, confidentiality issues, a denial of service, and remote code execution. **CVE-2023-46218** - This flaw allows a malicious HTTP server to set "super cookies" in curl that are then passed back to more origins than what is otherwise allowed or possible. This allows a site to set cookies that then would get sent to different and unrelated sites and domains. It could do this by exploiting a mixed case flaw in curl's function that verifies a given cookie domain against the Public Suffix List (PSL). F5 products can be vulnerable when custom scripts are used to accept super cookies and exposed to this vulnerability. F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	F5OS-A 1.4.0, 1.3.0 - 1.3.1 BIG-IP Next (all modules) 20.0.1 - 20.0.2 BIG-IP Next Central Manager 20.0.1 - 20.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000132893 https://my.f5.com/manage/s/article/K000138650

Affected Product	**Drupal**
Severity	**Low**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has released a security update addressing an Access Bypass vulnerability that exists in the Node Access Rebuild Progressive module. This module provides an alternative mean of rebuilding the Content Access table and it doesn't sufficiently reset the state of content access when the module is uninstalled. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Drupal Node Access Rebuild Progressive before 2.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-010

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.