Advisory Alert

Alert Number: AAA20240301 **Date:** March 1, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Race Condition Vulnerability
NetApp	**High**, Medium	Multiple Vulnerabilities
IBM	**Medium**	Security Update
F5	**Low**	Tcpdump Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-38371, CVE-2022-1471, CVE-2022-37452, CVE-2022-4244, CVE-2022-4245, CVE-2023-44487, CVE-2023-48795, CVE-2023-5072, CVE-2023-51766, CVE-2023-5678, CVE-2023-2650, CVE-2023-5868, CVE-2023-5870, CVE-2023-5869, CVE-2023-6378, CVE-2023-6481, CVE-2023-2454, CVE-2023-2455, CVE-2023-45322, CVE-2023-34055, CVE-2023-4039, CVE-2023-42794, CVE-2023-42795, CVE-2023-45648, CVE-2023-46589, CVE-2023-5717, CVE-2023-2137, CVE-2023-43643, CVE-2023-35116, CVE-2023-44483, CVE-2023-42114, CVE-2023-42115, CVE-2023-42116, CVE-2023-42117, CVE-2023-42118, CVE-2023-42119, CVE-2023-5535, CVE-2024-21626, CVE-2024-22457, CVE-2024-22458)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products that in turn affect dell products. An attacker may exploit these vulnerabilities which could lead to Plaintext recovery from cipher text and Server impersonation. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell Secure Connect Gateway Version 5.20.00.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222433/dsa-2024-076-security-update-for-dell-secure-connect-gateway-appliance-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Race Condition Vulnerability (CVE-2023-6546)
Description	Red Hat has released a security update addressing a Race Condition Vulnerability. This could allow a local unprivileged user to escalate their privileges on the system. 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 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1055

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-43937, CVE-2023-31423, CVE-2023-31424)
Description	NetApp has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2022-43937** - Brocade SANnav versions prior to v2.3.0 and 2.2.2a are susceptible to an information disclosure vulnerability. Sensitive fields are recorded in plaintext within the debug-enabled log files. Successful exploit requires an attacker to have access to debug-enabled log files. **CVE-2023-31423** - Brocade SANnav versions prior to v2.3.0 and 2.2.2a are susceptible to an information disclosure vulnerability. Sensitive fields are recorded in plaintext within the configuration log file when debugging is enabled. Successful exploit requires an attacker to have access to "supportsave" output. **CVE-2023-31424** - Brocade SANnav versions prior to v2.3.0 and 2.2.2a are susceptible to a vulnerability which could allow a remote unauthenticated attacker to bypass authentication and authorization in the Brocade SANnav web interface. NetApp recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Brocade SAN Navigator (SANnav) v2.3.0 and 2.2.2a
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240229-0005/ https://security.netapp.com/advisory/ntap-20240229-0003/ https://security.netapp.com/advisory/ntap-20240229-0004/

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2023-50312)
Description	IBM has released a security update for IBM WebSphere Application Server Liberty because it could provide weaker than expected security for outbound TLS connections. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Hybrid Edition 5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7127783

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	Tcpdump Vulnerability (CVE-2018-14880)
Description	F5 has released a security update addressing a Tcpdump Vulnerability. The vulnerability exist in OSPFv3 parser in tcpdump before 4.9.3, due to a buffer over-read in print-ospf6.c:ospf6_print_lshdr(). Exploitation of the vulnerability could allow an attacker gain access to sensitive information and can also cause a denial of service (DoS). F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) 15.0.0 - 15.1.2, 14.0.0 - 14.1.3, 13.1.0 - 13.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K56551263

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.