Advisory Alert

Alert Number: AAA20240823 **Date:** August 23, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SolarWinds	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Blast-RADIUS Vulnerability
IBM	**Critical**	Buffer Overflow Vulnerability
SonicWall	**High**	Improper Access Control Vulnerability
Dell	**High**	Multiple Vulnerabilities
F5	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
NetApp	**Medium**	Multiple Information Disclosure Vulnerabilities

Description

Affected Product	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28986, CVE-2024-28987)
Description	SolarWinds has released security updates addressing multiple vulnerabilities that exist in SolarWinds Web Help Desk. **CVE-2024-28986** - SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. **CVE-2024-28987** - The SolarWinds Web Help Desk (WHD) software is affected by a hardcoded credential vulnerability, allowing remote unauthenticated user to access internal functionality and modify data. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Web Help Desk 12.8.3 prior to Hotfix 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.solarwinds.com/SuccessCenter/s/article/SolarWinds-Web-Help-Desk-12-8-3-Hotfix-2

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Blast-RADIUS Vulnerability (CVE-2024-3596)
Description	NetApp has released security updates addressing the Blast-RADIUS Vulnerability that exists in Brocade Fabric Operating System and SAN Navigator. **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. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	RADIUS Protocol used in below • Brocade Fabric Operating System Firmware • Brocade SAN Navigator (SANnav)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240822-0001/

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2024-5564)
Description	IBM has released security updates addressing a Buffer Overflow Vulnerability that exists in IBM QRadar SIEM. **CVE-2024-5564** - libndp is vulnerable to a buffer overflow, caused by improper bounds checking by NetworkManager. By sending specially crafted IPV6 packets, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the application to crash. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP9 IF01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7166204

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2024-40766)
Description	SonicWall has released security updates addressing an Improper Access Control Vulnerability that exists in SonicOS management access. **CVE-2024-40766** - An improper access control vulnerability has been identified in the SonicWall SonicOS management access, potentially leading to unauthorized resource access and in specific conditions, causing the firewall to crash. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SonicWall Firewall Gen 5 devices running SonicOS 5.9.2.14-12o and older versions. SonicWall Firewall Gen 6 devices running SonicOS 6.5.4.14-109n and older versions. SonicWall Firewall Gen 7 devices running SonicOS 7.0.1-5035 and older versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27983, CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21144, CVE-2024-21131, CVE-2024-21138)
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 NetWorker Runtime Environment (NRE) Version 8.0.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227971/dsa-2024-367-security-update-for-dell-networker-runtime-environment-nre-security-vulnerabilities

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-1975, CVE-2024-7634)
Description	F5 has released workarounds addressing multiple vulnerabilities that exist in their products. **CVE-2024-1975** - If a server hosts a zone containing a "KEY" Resource Record, or a resolver DNSSEC-validates a "KEY" Resource Record from a DNSSEC-signed domain in cache, a client can exhaust resolver CPU resources by sending a stream of SIG(0) signed requests. This vulnerability allows a remote, unauthenticated attacker to cause a degradation of service that can lead to a denial-of-service (DoS) on the BIG-IP system. **CVE-2024-7634** - NGINX Agent's config_dirs restriction feature allows a highly privileged attacker to gain the ability to write/overwrite files outside of the designated secure directory. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (DNS) versions 15.1.0 - 15.1.10, 16.1.0 - 16.1.5 and 17.1.0 - 17.1.1 NGINX Agent versions 2.17.0 - 2.36.1 NGINX Instance Manager versions 2.3.1 - 2.17.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000140745 • https://my.f5.com/manage/s/article/K000140630

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar components. These vulnerabilities could be exploited to cause denial of service, sensitive information disclosure, arbitrary code execution, bypass security restrictions. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar DNS Analyzer App versions 1.0.0 - 2.0.1 IBM QRadar SIEM versions 7.5 - 7.5.0 UP9 IF01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7166213 • https://www.ibm.com/support/pages/node/7166204

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Multiple Information Disclosure Vulnerabilities (CVE-2024-29953, CVE-2024-29954)
Description	NetApp has released security updates addressing multiple Information Disclosure vulnerabilities that exist in their products. **CVE-2024-29953** - The Brocade Web Interface in Brocade Fabric OS versions prior to 9.2.1, v9.2.0b, and v9.1.1d prints encoded session passwords on session storage for Virtual Fabric platforms. This could allow an authenticated user to view other users' session encoded passwords. **CVE-2024-29954** - The password management API in Brocade Fabric OS versions prior to v9.2.1, v9.2.0b, v9.1.1d, and v8.2.3e prints sensitive information in log files. This could allow an authenticated user to view the server passwords for protocols such as scp and sftp. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• The Brocade Web Interface in Brocade Fabric OS versions prior to 9.2.1, v9.2.0b, and v9.1.1d • The password management API in Brocade Fabric OS versions prior to v9.2.1, v9.2.0b, v9.1.1d, and v8.2.3e
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20240822-0009/ • https://security.netapp.com/advisory/ntap-20240822-0010/

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.