Advisory Alert

Alert Number: **AAA20231107** **Date:** **November 7, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Veeam	**Critical**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
Veeam	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-14859, CVE-2019-14853, CVE-2019-0816, CVE-2020-8631, CVE-2020-8632, CVE-2016-1704)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities may lead to Information disclosure, Security feature bypass, Denial of Service, Malformed signature acceptance. Dell strongly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell NetWorker Virtual Edition - NetWorker Virtual Edition (NVE) • Versions 19.9, 19.9.0.1 • Versions 19.8 through 19.8.0.3 • Versions 19.7 through 19.7.0.5 • Version 19.7.1 • Versions prior to 19.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000219248/dsa-2023-056-security-update-for-dell-networker-virtual-edition-vulnerabilities

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38547, CVE-2023-38548)
Description	Veeam has released security updates addressing multiple vulnerabilities. **CVE-2023-38547**- A vulnerability in Veeam ONE allows an unauthenticated user to gain information about the SQL server connection Veeam ONE uses to access its configuration database. This may lead to remote code execution on the SQL server hosting the Veeam ONE configuration database. **CVE-2023-38548**- A vulnerability in Veeam ONE allows an unprivileged user who has access to the Veeam ONE Web Client the ability to acquire the NTLM hash of the account used by the Veeam ONE Reporting Service Veeam strongly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Veeam ONE 11, 11a, 12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4508

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1192, CVE-2023-1206, CVE-2023-1859, CVE-2023-2177, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-4155, CVE-2023-42753, CVE-2023-42754, CVE-2023-4389, CVE-2023-4563, CVE-2023-4622, CVE-2023-4623, CVE-2023-4881, CVE-2023-4921, CVE-2023-5345, CVE-2023-2163, CVE-2023-31085, CVE-2023-3111, CVE-2023-34324, CVE-2023-39189, CVE-2023-45862, CVE-2023-3777, CVE-2023-5178, CVE-2023-39191, CVE-2023-46813)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Privilege escalation, Denial of Service, Out of bounds reads, Arbitrary code execution. Suse recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20234072-2/ https://www.suse.com/support/update/announcement/2023/suse-su-20234377-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234378-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234375-1/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2068, CVE-2022-21426, CVE-2023-21830, CVE-2023-21843, CVE-2022-4304, CVE-2023-0215)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Denial of Service and Sensitive information disclosure. IBM recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	FOS 9.x prior to 9.2.0a SANnav 2.x prior to 2.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7067688 https://www.ibm.com/support/pages/node/7067690 https://www.ibm.com/support/pages/node/7067689 https://www.ibm.com/support/pages/node/7067691

Affected Product	**Veeam**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38549, CVE-2023-41723)
Description	Veeam has released security updates addressing multiple vulnerabilities. **CVE-2023-38549**- A vulnerability in Veeam ONE allows a user with the Veeam ONE Power User role to obtain the access token of a user with the Veeam ONE Administrator role through the use of XSS. **CVE-2023-41723**- A vulnerability in Veeam ONE allows a user with the Veeam ONE Read-Only User role to view the Dashboard Schedule. Veeam recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Veeam ONE 11, 11a, 12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4508

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.