Advisory Alert

Alert Number: AAA20230329 **Date:** March 29, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
OpenSSL	**Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2007-4559, CVE-2016-0682, CVE-2016-0689, CVE-2016-0694, CVE-2016-3418, CVE-2016-7103, CVE-2017-10140, CVE-2017-12613, CVE-2017-12814, CVE-2017-12837, CVE-2017-12883, CVE-2017-3604, CVE-2017-3605, CVE-2017-3606, CVE-2017-3607, CVE-2017-3608, CVE-2017-3609, CVE-2017-3610, CVE-2017-3612, CVE-2017-3613, CVE-2017-3614, CVE-2017-3615, CVE-2017-3616, CVE-2017-3617, CVE-2017-6004, CVE-2017-7186, CVE-2018-12015, CVE-2018-18074, CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314, CVE-2018-6797, CVE-2018-6798, CVE-2018-6913, CVE-2018-7160, CVE-2019-12749, CVE-2019-16869, CVE-2019-20444, CVE-2019-20445, CVE-2019-20838, CVE-2019-9512, CVE-2020-10543, CVE-2020-10650, CVE-2020-10663, CVE-2020-10735, CVE-2020-10878, CVE-2020-11080, CVE-2020-11612, CVE-2020-12723, CVE-2020-12762, CVE-2020-14152, CVE-2020-1752, CVE-2020-21595, CVE-2020-21596, CVE-2020-21597, CVE-2020-21598, CVE-2020-21600, CVE-2020-21601, CVE-2020-21602, CVE-2020-21603, CVE-2020-21604, CVE-2020-27216, CVE-2020-28196, CVE-2020-28491, CVE-2020-29361, CVE-2020-29363, CVE-2020-2981, CVE-2020-36179, CVE-2020-36180, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-36187, CVE-2020-36188, CVE-2020-36518, CVE-2020-6096, CVE-2020-7238, CVE-2021-20190, CVE-2021-22931, CVE-2021-22940, CVE-2021-23214, CVE-2021-28165, CVE-2021-31684, CVE-2021-3326, CVE-2021-33560, CVE-2021-33813, CVE-2021-35940, CVE-2021-35942, CVE-2021-36222, CVE-2021-3632, CVE-2021-36770, CVE-2021-37136, CVE-2021-37137, CVE-2021-3826, CVE-2021-38604, CVE-2021-3999, CVE-2021-4133, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42383, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386, CVE-2021-44531, CVE-2021-46848, CVE-2022-0778, CVE-2022-0891, CVE-2022-1245, CVE-2022-1271, CVE-2022-1292, CVE-2022-1552, CVE-2022-1586, CVE-2022-1587, CVE-2022-1941, CVE-2022-1996, CVE-2022-2068, CVE-2022-21824, CVE-2022-22576, CVE-2022-23219, CVE-2022-24999, CVE-2022-2509, CVE-2022-25235, CVE-2022-25236, CVE-2022-25314, CVE-2022-25315, CVE-2022-25857, CVE-2022-2625, CVE-2022-27775, CVE-2022-27782, CVE-2022-28321, CVE-2022-28805, CVE-2022-29162, CVE-2022-29241, CVE-2022-3171, CVE-2022-32212, CVE-2022-34169, CVE-2022-35256, CVE-2022-35737, CVE-2022-3602, CVE-2022-36049, CVE-2022-37454, CVE-2022-3782, CVE-2022-3786, CVE-2022-3970, CVE-2022-3996, CVE-2022-40149, CVE-2022-40150, CVE-2022-40303, CVE-2022-40304, CVE-2022-40674, CVE-2022-41881, CVE-2022-42003, CVE-2022-42004, CVE-2022-4262, CVE-2022-42898, CVE-2022-42915, CVE-2022-42919, CVE-2022-43548, CVE-2022-43680, CVE-2022-45061, CVE-2022-45146, CVE-2022-48281)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. Exploitation of the most severe vulnerabilities could lead to information disclosure, denial of service, malicious objection creation and potential information loss. Dell highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell Streaming Data Platform 1.1.x, 1.2.x, 1.3.x, 1.4.x, 1.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000211636/dsa-2023-086-dell-streaming-data-platform-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3523 ,CVE-2022-36280 ,CVE-2022-38096 ,CVE-2023-0045 ,CVE-2023-0122 ,CVE-2023-0266 ,CVE-2023-0461 ,CVE-2023-0590 ,CVE-2023-0597 ,CVE-2023-1075 ,CVE-2023-1076 ,CVE-2023-1078, CVE-2023-1095 ,CVE-2023-1118 ,CVE-2023-22995 ,CVE-2023-22998 ,CVE-2023-23000 ,CVE-2023-23001 ,CVE-2023-23004 ,CVE-2023-23454 ,CVE-2023-23455 ,CVE-2023-23559 ,CVE-2023-25012 ,CVE-2023-26545,CVE-2023-26545 ,CVE-2023-28328)
Description	Suse has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to use-after-free condition, privilege escalation, heap out-of-bounds write and double free condition. Suse recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	openSUSE Leap 15.4 openSUSE Leap Micro 5.3 Public Cloud Module 15-SP4 SUSE Linux Enterprise High Performance Computing 12 SP4, 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 12-SP4, 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12-SP4, 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Server for SAP Applications 12-SP4, 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3 SUSE Real Time Module 15-SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20231610-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231609-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231605-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231602-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231599-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231595-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231608-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231635-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231621-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231619-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231639-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231645-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231647-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231640-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231653-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231654-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231651-1 https://www.suse.com/support/update/announcement/2023/suse-su-20231649-1

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0465, CVE-2023-0466)
Description	OpenSSL has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2023-0465**- The OpenSSL policy checking mechanisms silently ignore any invalid certificate policies present in the leaf certificates, thereby skipping other related checks. This scenario can be exploited by a malicious certification authority (CA) to deliberately assert invalid certificate policies to evade policy checking altogether. **CVE-2023-0466**- The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However, in practice, the implementation of this function does not activate the check, which can result in invalid or incorrect certificates passing verification. As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument. Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications. OpenSSL recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	OpenSSL 3.1, 3.0, 1.1.1 and 1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230328.txt

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.