Advisory Alert

Alert Number: **AAA20221108** **Date:** **November 8, 2022**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Debian	**Critical**	SQL Injection Vulnerability
Splunk	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Debian	**High**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Debian**
Severity	**Critical**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2022-28346)
Description	An SQL injection vulnerability exists in python-django (PTS) framework used by Debian. Successful exploitation of this vulnerability allows an attacker to execute SQL injection via crafted dictionary expansion.
Affected Products	python-django (PTS) 1:1.11.29-1~deb10u1 python-django (PTS) 2:2.2.26-1~deb11u1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security-tracker.debian.org/tracker/CVE-2022-28346

Affected Product	**Splunk**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36518, CVE-2022-43572, CVE-2022-43571, CVE-2022-43570, CVE-2022-43569, CVE-2022-43568)
Description	Splunk has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause denial of service, arbitrary code execution, cross-site scripting (XSS) and extensible markup language (XML) external entity (XXE) injection via a custom View. Splunk highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Splunk Enterprise 8.1.11 and lower Splunk Enterprise 8.2.0 to 8.2.8 Splunk Enterprise 9.0.0 to 9.0.1 Splunk Cloud Platform 9.0.2203.4 and lower Splunk Cloud Platform 9.0.2208 and lower Splunk Cloud Platform 9.0.2209 and lower
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1113.html https://www.splunk.com/en_us/product-security/announcements/svd-2022-1112.html https://www.splunk.com/en_us/product-security/announcements/svd-2022-1111.html https://www.splunk.com/en_us/product-security/announcements/svd-2022-1110.html https://www.splunk.com/en_us/product-security/announcements/svd-2022-1109.html https://www.splunk.com/en_us/product-security/announcements/svd-2022-1108.html

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3618, CVE-2022-43995, CVE-2022-43680)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2021-3618** - A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer. **CVE-2022-43995** - Sudo 1.8.0 through 1.9.12, with the crypt() password backend, contains a plugins/sudoers/auth/passwd.c array-out-of-bounds error that can result in a heap-based buffer over-read. This can be triggered by arbitrary local users with access to Sudo by entering a password of seven characters or fewer. **CVE-2022-43680** - In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations. Suse highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	SUSE Linux Enterprise Server 12-SP5 SUSE Linux Enterprise Server 12-SP2-BCL SUSE Linux Enterprise Desktop 15-SP4 SUSE Linux Enterprise High Performance Computing 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Module for Basesystem 15-SP4 SUSE Linux Enterprise Server 15-SP4 SUSE Linux Enterprise Server for SAP Applications 15-SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3 openSUSE Leap 15.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2022/suse-su-20223888-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223886-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223884-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2928, CVE-2022-2929, CVE-2020-15503, CVE-2020-35531, CVE-2020-35533, CVE-2020-35532, CVE-2020-35530)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause denial of service, arbitrary code execution and server crash. Ubuntu highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Ubuntu 20– versions prior to Ubuntu 20.04 Ubuntu 18– versions prior to Ubuntu 18.04 Ubuntu 16– versions prior to Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5658-2 https://ubuntu.com/security/notices/USN-5715-1

Affected Product	**Debian**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-23239, CVE-2022-2996, CVE-2022-44638, CVE-2021-45115, CVE-2021-45116)
Description	Debian has released security updates addressing multiple vulnerabilities that exist in their products. Attackers could exploit these vulnerabilities to cause arbitrary code execution, Man-in-the-middle (MITM) attacks, heap-based buffer overflow, denial of service and information discloser. Debian highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	python-django (PTS) 1:1.11.29-1~deb10u1 pixman (PTS) 0.36.0-1, 0.40.0-1 python-scciclient (PTS) 0.7.2-2, 0.8.0-2 sudo (PTS) 1.8.27-1+deb10u3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.debian.org/lts/security/2022/dla-3181 https://www.debian.org/lts/security/2022/dla-3180 https://www.debian.org/lts/security/2022/dla-3179 https://www.debian.org/lts/security/2022/dla-3177

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.