Advisory Alert

Alert Number: AAA20230109 **Date:** January 9, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Debian	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-4159,CVE-2022-0171,CVE-2022-20421,CVE-2022-26365,CVE-2022-2663,CVE-2022-3061,CVE-2022-3303,CVE-2022-33743,CVE-2022-3524,CVE-2022-3541, CVE-2022-3543,CVE-2022-3544,CVE-2022-3564,CVE-2022-3566,CVE-2022-3567,CVE-2022-3586,CVE-2022-3594,CVE-2022-3621,CVE-2022-3623,CVE-2022-3646,CVE-2022-3649,CVE-2022-37290,CVE-2022-3910,CVE-2022-39188,CVE-2022-3977,CVE-2022-39842,CVE-2022-40307,CVE-2022-4095,CVE-2022-41849,CVE-2022-41850,CVE-2022-42703,CVE-2022-43551, CVE-2022-43552,CVE-2022-43750,CVE-2022-43945,CVE-2022-47629)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities can lead to denial of service, arbitrary code execution or expose sensitive information. Ubuntu highly recommends to apply necessary fixes to avoid issues.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 22.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5793-1 https://ubuntu.com/security/notices/USN-5792-1 https://ubuntu.com/security/notices/USN-5791-1 https://ubuntu.com/security/notices/USN-5790-1 https://ubuntu.com/security/notices/USN-5789-1 https://ubuntu.com/security/notices/USN-5788-1 https://ubuntu.com/security/notices/USN-5787-1 https://ubuntu.com/security/notices/USN-5786-1

Affected Product	**Debian**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2018-25047, CVE-2022-4121)
Description	Debian has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities can lead to cross-site scripting and null pointer dereference. **CVE-2018-25047–** There was a potential cross-site scripting vulnerability in smarty3, a widely-used PHP templating engine. libs/plugins/function.mailto.php allows XSS in the vulnerable Smarty engine. A web page that uses smarty_function_mailto and that could be parameterized using GET or POST input parameters could allow injection of JavaScript code by a user. **CVE-2022-4121–** There was a potential null pointer dereference vulnerability in libetpan, a low-level library for handling emails. The null pointer is present at mailimap_mailbox_data_status_free in low-level/imap/mailimap_types.c. Debian recommends to apply necessary fixes to avoid issues.
Affected Products	Debian libetpan (PTS) buster version 1.9.3-2+deb10u1 Debian libetpan (PTS) bullseye version 1.9.4-3 Debian smarty3 (PTS) buster version 3.1.33+20180830.1.3a78a21f+selfpack1-1+deb10u1 Debian smarty3 (PTS) bullseye (security), bullseye version 3.1.39-2+deb11u1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.debian.org/lts/security/2023/dla-3262 https://www.debian.org/lts/security/2023/dla-3261

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.