Advisory Alert

Alert Number: AAA20221028 **Date:** October 28, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**High**	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33060, CVE-2021-23133, CVE-2021-22555, CVE-2019-18197)
Description	F5 has released patch updates to addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could leads to privilege escalation, Denial of service and unauthorized data disclosure. F5 highly recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	F5OS-A version 1.1.1 - 1.2.0 F5 BIG-IP (all modules) versions - 15.1.0 - 15.1.7 F5 Traffix SDC version 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.f5.com/csp/article/K12055286 https://support.f5.com/csp/article/K67416037 https://support.f5.com/csp/article/K06524534 https://support.f5.com/csp/article/K10812540

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42010, CVE-2022-42011, CVE-2022-42012, CVE-2022-3570, CVE-2022-3598)
Description	Ubuntu has released a security update addressing the multiple vulnerabilities that exist in the DBus and the LibTIFF libraries. Successful exploitation of these vulnerabilities could cause denial of service, application crash and information disclosure. Ubuntu highly recommends to apply the available updates at your earliest to avoid issues.
Affected Products	D-Bus versions before 1.12.24, 1.13.x 1.14.x before 1.14.4, and 1.15.x before 1.15.2. LibTIFF 4.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5704-1 https://ubuntu.com/security/notices/USN-5705-1

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.