Advisory Alert

Alert Number: AAA20221219 **Date:** December 19, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Remote Code Execution Vulnerability
Ubuntu	**High**	Use-after-free vulnerability
SUSE	**High**	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Denial of Service Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2017-12240)
Description	Cisco has released an update for a security update that was released earlier, addressing a critical remote code execution vulnerability that exist in Cisco IOS and Cisco IOS XE Software. **CVE-2017-12240** – This vulnerability exists due to a buffer overflow condition in the DHCP relay subsystem of the affected software. An attacker could exploit this vulnerability by sending a crafted DHCP Version 4 (DHCPv4) packet to an affected system. A successful exploit could allow the attacker to execute arbitrary code and gain full control of the affected system or cause the affected system to reload, resulting in a DoS condition. Cisco highly recommends to apply the patch updates at the earliest to avoid issues.
Affected Products	Cisco devices that are running a vulnerable release of Cisco IOS Software or Cisco IOS XE Software and are configured as a DHCP relay agent
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-dhcp

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Use-after-free vulnerability (CVE-2022-42896)
Description	Ubuntu has released a security update to address a use-after-free vulnerability that exists in the Linux kernel. **CVE-2022-42896** - Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. Ubuntu highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 22.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5783-1

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2602, CVE-2022-28693, CVE-2022-3567 , CVE-2022-3628 , CVE-2022-3635, CVE-2022-3707, CVE-2022-3903, CVE-2022-4095, CVE-2022-4129, CVE-2022-4139, CVE-2022-41850, CVE-2022-41858, CVE-2022-42895, CVE-2022-42896, CVE-2022-4378, CVE-2022-43945, CVE-2022-45934, CVE-2022-3176, CVE-2022-3566, CVE-2022-3643, CVE-2022-42328, CVE-2022-42329, CVE-2022-45869, CVE-2022-45888, CVE-2022-4378, CVE-2022-43945, CVE-2022-3545, CVE-2022-3586, CVE-2022-41218, CVE-2022-3577, CVE-2022-3640, CVE-2022-2964, CVE-2022-3545 CVE-2021-39698)
Description	SUSE has released a security update to address multiple vulnerabilities that exists in their products and, packagers that used by their products. Successful exploitation of the most severe vulnerabilities could cause buffer overflow, denial of service, information leakage and creates a race condition in the kernel. SUSE highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	OpenSUSE Leap 15.3, 15.4 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Performance Computing 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Live Patching 12-SP4, 12-SP5 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Module for Live Patching 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Public Cloud 15-SP3, 15-SP4 SUSE Linux Enterprise Server 12-SP5 SUSE Linux Enterprise Server 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Server for SAP Applications 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Manager Proxy 4.2, 4.3 SUSE Manager Retail Branch Server 4.2, 4.3 SUSE Manager Server 4.2, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Denial of Service Vulnerabilities (CVE-2017-12235, CVE-2017-12237, CVE-2017-12232, CVE-2017-6627, CVE-2017-12231, CVE-2017-12233, CVE-2017-12234, CVE-2017-12319)
Description	Cisco has released an update for set of security updates that was released earlier, addressing multiple vulnerabilities that exist in their products. Successful exploitation of this vulnerabilities could leads to denial of service. Cisco highly recommends to apply the patch updates at the earliest to avoid issues.
Affected Products	Multiple Products and versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-profinet https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ike https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-rbip-dos https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-ios-udp https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-nat https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171103-bgp https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-cip

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.