Advisory Alert

Alert Number: AAA20221129 **Date:** November 29, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Insufficient Access Control Vulnerability
Redhat	**High**	Security Update
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
IBM	**Medium**	Denial of service Vulnerability

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Insufficient Access Control Vulnerability (CVE-2022-20956)
Description	Cisco has released a security update to address an Insufficient Access Control Vulnerability that exists in the web-based management interface of the Cisco Identity Services Engine. A remote attacker can bypass authorization and access system files on an affected device by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to list, download, and delete certain files that they should not have access to. Cisco recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	Cisco ISE 3.1 Cisco ISE 3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2019-8331, CVE-2021-3717, CVE-2021-31684, CVE-2021-44906, CVE-2022-0613, CVE-2022-2048, CVE-2022-2053, CVE-2022-24723, CVE-2022-24785, CVE-2022-24823, CVE-2022-25857, CVE-2022-31129, CVE-2022-31197, CVE-2022-33980, CVE-2022-38749, CVE-2022-41853, CVE-2022-42889)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in Redhat Fuse. Successful exploitation of the vulnerabilities could lead to an RCE attack, SQL injection, Denial of service, Prototype pollution, Authorization bypass, and Path traversal. Redhat recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	Red Hat Fuse 1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:8652

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-2626, CVE-2013-4235, CVE-2020-16156, CVE-2015-9274)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in their Products and packages. Successful exploitation of these vulnerabilities could lead to privilege escalation, race condition, signature bypass and denial of service. Ubuntu recommends to apply the necessary updates at your earliest to avoid issues.
Affected Products	Ubuntu 18.04 Ubuntu 16.04 Ubuntu 22.10 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5744-1 https://ubuntu.com/security/notices/USN-5745-1 https://ubuntu.com/security/notices/USN-5689-2 https://ubuntu.com/security/notices/USN-5746-1

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Denial of service Vulnerability (CVE-2022-3171, CVE-2022-3509)
Description	IBM has released security updates addressing a denial of service vulnerability that exists in IBM WebSphere Application Server Liberty. **CVE-2022-3171**- protobuf-java core and lite are vulnerable to a denial of service, caused by a flaw in the parsing procedure for binary and text format data. By sending non-repeated embedded messages with repeated or unknown fields, a remote authenticated attacker could exploit this vulnerability to cause long garbage collection pauses. **CVE-2022-3509**- protobuf-java core and lite are vulnerable to a denial of service, caused by a flaw in the parsing procedure for textformat data. By sending non-repeated embedded messages with repeated or unknown fields, a remote authenticated attacker could exploit this vulnerability to cause long garbage collection pauses. IBM recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server Liberty 21.0.0.2 - 22.0.0.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6841889

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.