Advisory Alert

Alert Number: AAA20211021 **Date:** October 21, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	Multiple vulnerabilities
IBM QRadar Advisor	**Critical**	Multiple vulnerabilities
Cisco	**High, Medium**	Multiple vulnerabilities

Description

Affected Product	Oracle
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities
Description	Oracle has released its October 2021 Security Updates which address multiple Vulnerabilities across several of products, which an attacker could use to gain control of an affected system. Oracle highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpuoct2021.html

Affected Product	IBM QRadar Advisor
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2020-36242, CVE-2021-33503, CVE-2020-28493)
Description	IBM has released Security Updates addressing multiple vulnerabilities that exists in IBM QRadar Advisor. **CVE-2020-36242 -** An integer overflow and a buffer overflow in cryptography could allow a remote attacker to execute arbitrary code on the system. **CVE-2021-33503 -** A vulnerability in urllib3 has been found that could allow an attacker to cause a denial of service (DDoS) via a specially-crafted URL request. **CVE-2020-28493 -** Pallets jinja2 is vulnerable to a denial of service (DoS) attack. Remote attackers could exploit this vulnerability by sending a specially-crafted input to the Jinja2 database. IBM highly recommends to apply necessary fixes to the products at earliest to avoid issues.
Affected Products	QRadar Advisor 2.5 - QRadar Advisor 2.6.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6507113

Affected Product	Cisco
Severity	**High, Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-1529, CVE-2021-34737, CVE-2021-34743, CVE-2021-34738, CVE-2021-40121, CVE-2021-40123, CVE-2021-34736)
Description	Cisco has released security patch updates addressing multiple vulnerabilities that exists in multiple Cisco products. An attacker could use these vulnerabilities to gain access to systems and perform Command Injection, Denial of Service, Authorization Bypass, Cross-Site Scripting, File Download Vulnerability malicious activities. Most of the vulnerabilities are found in the Cisco IOS XE SD-WAN, Cisco IOS XR Software, Cisco Webex, Cisco Identity Services Engine.
Affected Products	Cisco IOS XE SD-WAN Cisco IOS XR Software Cisco Webex Cisco Identity Services Engine Cisco Integrated Management
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dhcp-dos-pjPVReLU https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-2FmKd7T https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss1-rgxYry2V https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-download-B3BR5KQA https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh

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.