Advisory Alert

Alert Number : AAA20201008 **Date :** October 8, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM QRadar SIEM	**High**	Multiple Vulnerabilities
CISCO	**High**	Multiple Vulnerabilities

Description

Affected Product	IBM QRadar SIEM
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has release patch updates for multiple vulnerabilities in QRadar Security Information and Event Management system. Addressed vulnerabilities include man-in-the-middle attacks, denial of service attacks, executing arbitrary commands and injecting malicious scripts which could allow an unauthenticated attacker to gain access to a compromised systems.
Affected Products	IBM QRadar SIEM 7.4.0 – 7.4.1 IBM QRadar SIEM 7.3.0 – 7.3.3 IBM QRadar Incident Forensics 7.4.0 – 7.4.1 IBM QRadar Incident Forensics 7.3.0 – 7.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6344071 https://www.ibm.com/support/pages/node/6344081 https://www.ibm.com/support/pages/node/6344075 https://www.ibm.com/support/pages/node/6344079

Affected Product	CISCO
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3568) , (CVE-2020-3467) , (CVE-2020-3589) , (CVE-2020-3536) (CVE-2020-3597) , (CVE-2020-3567) , (CVE-2020-3320) , (CVE-2020-3602) , (CVE-2020-3601)
Description	CISCO has released security updates addressed multiple vulnerabilities that exists in multiple products. **CVE-2020-3568** : Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. **CVE-2020-3467 & CVE-2020-3589** : Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to modify parts of the configuration and Web-based management Software could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. **CVE-2020-3536** : Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. **CVE-2020-3597** : Cisco Nexus Data Broker software could allow an unauthenticated, remote attacker to perform a directory traversal attack on an affected device **CVE-2020-3567** : Cisco Industrial Network Director (IND) could allow an authenticated, remote attacker to cause the CPU utilization to increase to 100 percent, resulting in a denial of service (DoS) condition on an affected device **CVE-2020-3320** : Cisco Firepower Management Center could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user interface. **CVE-2020-3602 & CVE-2020-3601** : Cisco ASR 5000 Series Routers could allow an authenticated, local attacker to elevate privileges on an affected device.
Affected Products	Cisco ESA releases 13.5.2 and earlier Cisco ISE Software, 2.2p16, 2.3p7, 2.4p12, 2.6p7, 2.7p2 and earlier Cisco vManage Software 20.1.2 and 20.3.1 and earlier Cisco Nexus Data Broker 3.9 and earlier. Cisco IND releases 1.9.0 and later Cisco Firepower Management 6.6.1 and earlier Cisco ASR 5000 Series Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x

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.