Advisory Alert

Alert Number: AAA20201117 **Date:** November 17, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-27130 , CVE-2020-27125 , CVE-2020-27131)
Description	**CVE-2020-27130** - This vulnerability could allow an unauthenticated, remote attacker to gain access to sensitive information. An attacker sending a crafted request allows the attacker to download arbitrary files from the affected device. **CVE-2020-27125** - This vulnerability could allow an unauthenticated, remote attacker to access sensitive information on an affected system. Due to insufficient protection of static credentials, an attacker could exploit this vulnerability by viewing source code by a successful exploiting, which the attacker could use to carry out further attacks. **CVE-2020-27131** - These Multiple vulnerabilities in the Java deserialization function that is used for an unauthenticated, remote attacker to execute arbitrary commands on an affected device. An attacker could exploit by sending a malicious serialized Java object to a specific listener. A successful exploit allows the attacker to execute arbitrary commands on an affected system.
Affected Products	Cisco Security Manager releases 4.21 and earlier.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-path-trav-NgeRnqgR https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-rce-8gjUz9fW https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-java-rce-mWJEedcD

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.