Advisory Alert

Alert Number: AAA20210713 **Date:** July 13, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	**Multiple Vulnerabilities**
Apache	**High**	**HTTP request smuggling**

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-1858, CVE-2019-1735, CVE-2019-1728)
Description	Cisco has released security patch updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could cause Denial of Service, Command Injection and Secure Configuration Bypass effects on the systems. Cisco secure highly recommends to apply necessary security fixes to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-snmp-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-cmdinj-1735 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-conf-bypass

Affected Product	Apache
Severity	**High**
Affected Vulnerability	HTTP request smuggling (CVE-2021-33037)
Description	Apache Tomcat did not correctly parse the HTTP transfer encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Apache recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Apache Tomcat 10.0.0-M1 to 10.0.6 Apache Tomcat 9.0.0.M1 to 9.0.46 Apache Tomcat 8.5.0 to 8.5.66
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tomcat.apache.org/security-10.html https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-8.html

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.