Advisory Alert

Alert Number : AAA20210118 **Date :** January 18, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Apache	**High**	Information Disclosure
Jenkins	**High**	Multiple Vulnerabilities
PaloAlto	**Medium**	Multiple Vulnerabilities

Description

Affected Product	Apache
Severity	**High**
Affected Vulnerability	Information Disclosure (CVE-2021-24122)
Description	Apache has released security patch updates addressing multiple vulnerabilities that exists in their products. Due to a flaw that exists in Apache it was possible to bypass security constraints and/or view the source code for JSPs in some configurations while serving resources from a network location using the NTFS file system. This is caused by the unexpected behavior of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behavior of the Windows API (FindFirstFileW) in some circumstances.
Affected Products	Apache Tomcat 10.0.0-M1 to 10.0.0-M9 Apache Tomcat 9.0.0.M1 to 9.0.39 Apache Tomcat 8.5.0 to 8.5.59 Apache Tomcat 7.0.0 to 7.0.106
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 https://tomcat.apache.org/security-7.html

Affected Product	Jenkins
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-21603, CVE-2021-21608, CVE-2021-21610 , CVE-2021-21611, CVE-2021-21604, CVE-2021-21602, CVE-2021-21605, CVE-2021-21606, CVE-2021-21607, CVE-2021-21609, CVE-2021-21612, CVE-2021-21613, CVE-2021-21614)
Description	Jenkins has released security patch updates addressing multiple vulnerabilities that exists in their products. It is recommended by Jenkins to apply necessary fixes according to the products used at earliest to avoid issues.
Affected Products	Jenkins weekly up to and including 2.274 Jenkins LTS up to and including 2.263.1 Bumblebee HP ALM Plugin up to and including 4.1.5 TICS Plugin up to and including 2020.3.0.6 TraceTronic ECU-TEST Plugin up to and including 2.23.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.jenkins.io/security/advisory/2021-01-13/

Affected Product	PaloAlto
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	CVE-2021-3031 – An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This vulnerability is caused since the padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created which leads to leaking of small amount of random information from the firewall memory into the Ethernet packets. CVE-2021-3032 - Configuration secrets for the “http”, “email”, and “snmptrap” v3 log forwarding server profiles can be logged to the logrcvr.log system log due to an information exposure through log file vulnerability that exists in Palo Alto Networks PAN-OS software. Logged information may include up to 1024 bytes of the configuration including the username and password in an encrypted form and private keys used in any certificate profiles set for log forwarding server profiles.
Affected Products	PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1. All versions of PAN-OS 8.0 and PAN-OS 7.1.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2021-3031 https://security.paloaltonetworks.com/CVE-2021-3032

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.