Advisory Alert

Alert Number : AAA20200701 **Date :** July 1, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Apache Tomcat	**High**	Denial of Service
Palo Alto	**High**	Authentication Bypass in SAML Authentication
IBM WebSphere Application Server	**High**	Denial of Service
IBM Db2	**High**	Privilege Escalation

Description

Affected Product	Apache Tomcat
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2020-11996)
Description	Multiple Apache Tomcat versions can be used by an attacker to trigger high CPU usage for several seconds using an specially crafted sequence of HTTP/2 requests. And the server could become unresponsive when several HTTP/2 requests are made simultaneously.
Affected Products	Apache Tomcat 10.0.0-M1 to 10.0.0-M5 Apache Tomcat 9.0.0.M1 to 9.0.35 Apache Tomcat 8.5.0 to 8.5.55
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	http://tomcat.apache.org/security-10.html http://tomcat.apache.org/security-9.html http://tomcat.apache.org/security-8.html

Affected Product	Palo Alto
Severity	**High**
Affected Vulnerability	Authentication Bypass in SAML Authentication (CVE-2020-2021)
Description	Resources (GlobalProtect Gateway, GlobalProtect Portal, GlobalProtect Clientless VPN, Authentication and Captive Portal,PAN-OS next-generation firewalls (PA-Series, VM-Series) and Panorama web interfaces, Prisma Access) using SAML authentication are affected by improper verification of signatures in PAN-OS SAML if the "Validate identity provider certificate" option is set to "disabled". It could allow an unauthenticated network-based attacker to access protected resources and perform administrative actions.
Affected Products	PAN-OS 9.1.3 PAN-OS 9.0.9 PAN-OS 8.1.15 PAN-OS 8.0.*
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2020-2021
Affected Product	IBM WebSphere Application Server

Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2019-12406)
Description	Apache CXF versions before 3.3.4 and 3.2.11 used by IBM WebSphere Application Server are vulnerable since it doesn't have a default limit for the number of message attachments to be included in a given message. This weakness can be used by an attacker to cause a denial of service attack by crafting a message with a large number of message attachments.
Affected Products	IBM Tivoli Netcool Impact 7.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6241360

Affected Product	IBM Db2
Severity	**High**
Affected Vulnerability	Privilege Escalation (CVE-2020-4204)
Description	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) could cause a buffer overflow due to improper bounds checking. It could allow a local attacker to escalate privileges and execute arbitrary codes on the system as an authenticated root user.
Affected Products	IBM Db2 V9.7, V10.1, V10.5, V11.1, V11.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/2875875

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.