Advisory Alert

Alert Number: AAA20210302 **Date:** March 2, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Buffer overflow
Tomcat	**High , Low**	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Buffer overflow (CVE-2020-8625)
Description	Redhat released updates addressing a buffer overflow in BIND. This flaw was found in the SPNEGO implementation. TSIG protocol which is intended to support the secure exchange of keys for use in verifying the authenticity of communications between parties on a network. It is a negotiation mechanism used by GSSAPI, the application protocol interface for GSS-TSIG. The most likely outcome of a successful exploitation of the vulnerability is a crash of the named process or possibly perform remote code execution. However the vulnerability can be avoided by choosing not to enable the use of GSS-TSIG features..
Affected Products	Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 8 Red Hat Enterprise Linux 8.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:0672 https://access.redhat.com/errata/RHSA-2021:0671 https://access.redhat.com/errata/RHSA-2021:0669 https://access.redhat.com/errata/RHSA-2021:0670 https://access.redhat.com/security/cve/CVE-2020-8625?extIdCarryOver=true&sc_cid=701f2000001OH6kAAG

Affected Product	**Tomcat**
Severity	CVE-2021-25122 - **High** , CVE-2021-25329 - **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-25329, CVE-2021-25122)
Description	Tomcat released security patch updates addressing Multiple Vulnerabilities. **CVE-2021-25329 -** The fix for CVE-2020-9484 was incomplete. When using a highly unlikely configuration edge case, the Tomcat instance was still vulnerable to CVE-2020-9484 (CVE-2020-9484 - An attacker is able to control the contents and name of a file on the server is Configured to use the PersistenceManager. A sufficiently lax filter to allow the attacker provided Object to be desterilized and the attacker knows the relative file path from the storage location used by FileStore. Then using a specifically crafted request attacker will be able to trigger remote code execution via deserialization of the file under their control.) **CVE-2021-25122 -** When responding to new h2c connection requests Apache Tomcat versions are could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request
Affected Products	Apache Tomcat 10.0.0-M1 to 10.0.0 Apache Tomcat 9.0.0.M1 to 9.0.41 Apache Tomcat 8.5.0 to 8.5.61 Apache Tomcat 7.0.0 to 7.0.107
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

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.