Advisory Alert

Alert Number : AAA20200812 **Date :** August 12, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Vulnerabilities
Red Hat	**High**	Denial Of Service
VMware	**High**	Privilege Escalation

Description

Affected Product	Microsoft
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released its August 2020 Security Updates which address multiple vulnerabilities across several of products, Which an attacker could use to gain control of an affected system.
Affected Products	Microsoft Windows Microsoft Edge (EdgeHTML-based) Microsoft Edge (Chromium-based) Internet Explorer Microsoft Scripting Engine SQL Server Microsoft JET Database Engine .NET Framework ASP.NET Core Microsoft Office and Microsoft Office Services and Web Apps Microsoft Windows Codecs Library Microsoft Dynamics
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Aug

Affected Product	Red Hat
Severity	**High**
Affected Vulnerability	Denial Of Service (CVE-2020-13935)
Description	Apache tomcat does not validate the payload length of the web socket framework. This issue has been identified in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could create an infinite loop which will eventually lead to a Denial of Service.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2020:3382 https://access.redhat.com/security/cve/CVE-2020-13935

Affected Product	VMware
Severity	**High**
Affected Vulnerability	Privilege Escalation (CVE-2020-3974)
Description	VMware has released their security updates to address a privilege escalation vulnerability due to improper XPC Client validation that affects multiple VMware products. Successful exploitation of this will allow attackers with normal user privileges to escalate their privileges to root on the system.
Affected Products	VMware Fusion Pro / Fusion VMware Remote Console for Mac (VMRC for Mac) VMware Horizon Client for Mac
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0017

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.