



# Advisory Alert

Alert Number: AAA20201030

Date: October 30, 2020

Document Classification Level : **Public Circulation Permitted**Information Classification Level : **TLP: WHITE**

## Overview

Product	Severity	Vulnerability
Microsoft	<b>Critical</b>	CVE-2020-1472: Elevation of privilege (AAA20200812)
Oracle	<b>Critical</b>	CVE-2020-14882: Remote code execution (AAA20201021)

## Description

Affected Product	Microsoft
Severity	<b>Critical</b> - Initial release date is 12th Aug 2020. This patch is again sent as a reminder to update since there are recent exploitation attempts of this vulnerability throughout the world.
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	<a href="https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Aug">https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Aug</a>

Affected Product	Oracle
Severity	<b>Critical</b> - Initial release date is 21st Oct 2020. This patch is again sent as a reminder to update since there are recent exploitation attempts of this vulnerability throughout the world.
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released its October 2020 Critical patch update containing a collection of patches to address several security vulnerabilities affected by multiple products.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.oracle.com/security-alerts/cpuoct2020.html">https://www.oracle.com/security-alerts/cpuoct2020.html</a>

## 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.