Advisory Alert

Alert Number : AAA20201014 **Date :** October 14, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Vulnerabilities

Description

Affected Product	Microsoft
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-16889, CVE-2020-16896, CVE-2020-16897, CVE-2020-16901, CVE-2020-16904, CVE-2020-16914, CVE-2020-16918, CVE-2020-16919, CVE-2020-16921, CVE-2020-16928, CVE-2020-16929, CVE-2020-16930, CVE-2020-16931, CVE-2020-16932, CVE-2020-16933, CVE-2020-16934, CVE-2020-16937, CVE-2020-16938, CVE-2020-16941, CVE-2020-16942, CVE-2020-16947, CVE-2020-16949, CVE-2020-16954, CVE-2020-16955, CVE-2020-16957, CVE-2020-16969, CVE-2020-16995)
Description	Microsoft released security patch updates for multiple vulnerabilities that has been discovered in their products, the most severe flaw of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could lead an attacker gaining the same privileges as an authorized user. Depending on the privileges associated with the user, an attacker could then install programs, view, modify, delete data or create new accounts with administrative access. Users whose accounts are configured to have low access rights on the system could be less impacted than those who operate with administrative user rights. Microsoft highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Microsoft Windows Microsoft Office and Microsoft Office Services and Web Apps Microsoft JET Database Engine Azure Functions Open Source Software Microsoft Exchange Server Visual Studio PowerShellGet Microsoft .NET Framework Microsoft Dynamics Adobe Flash Player Microsoft Windows Codecs Library
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Oct

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.