Advisory Alert

Alert Number : **AAA20200610** **Date :** **June 10, 2020**

Document Classification Level **:** Public Circulation Permitted

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Vulnerabilities
Zimbra	**High**	Remote Code Execution
NTP	**High**	Denial of service

Description

Affected Product	**Microsoft**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released its June 2020 Security Updates which addresses multiple vulnerabilities across several of its 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) in IE Mode Internet Explorer Microsoft office and Microsoft Office Services and Web Apps Windows Defender Microsoft Dynamics Visual Studio Azure DevOps Adobe Flash Player Microsoft Apps for Android Windows App Store System Centre Android App
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Jun

Affected Product	Zimbra
Severity	**High**
Affected Vulnerability	Remote Code Execution
Description	A Remote code execution vulnerability was found in Zimbra Collaboration Suite. That could allow an attacker to compromise and remotely perform arbitrary actions on an affected system.
Affected Products	Prior to update 8.8.15 Patch 10 Prior to update 9.0.0 Patch 3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Security_Center https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P3#Security_Fixes

Affected Product	Network Time Protocol
Severity	High
Affected Vulnerability	Denial of service
Description	Exploitation of these vulnerability may allow a remote attacker to cause of denial of service condition.
Affected Products	Prior to update ntp-4.2.8p14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	http://support.ntp.org/bin/view/Main/NtpBug3596 https://bugs.ntp.org/show_bug.cgi?id=3596

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.