Advisory Alert

Alert Number: AAA20201209 **Date:** December 9, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Vulnerabilities
Apache Struts 2	**High**	Remote code execution
OpenSSL	**High**	Denial of service

Description

Affected Product	Microsoft
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released its December 2020 Security Updates which address multiple vulnerabilities across several of products, Which an attacker could use to gain control of an affected system. Microsoft highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Microsoft Windows Microsoft Edge (EdgeHTML-based) Microsoft Edge for Android ChakraCore Microsoft Office and Microsoft Office Services and Web Apps Microsoft Exchange Server Azure DevOps Microsoft Dynamics Visual Studio Azure SDK Azure Sphere
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2020-Dec

Affected Product	Apache Struts 2
Severity	**High**
Affected Vulnerability	Remote code execution (CVE-2020-17530)
Description	A vulnerability has been identified in Apache Struts 2. A remote attacker can exploit this vulnerability to perform remote code execution and security restriction bypass on the targeted system. Apache has recommends Upgrade to Struts 2.5.26 or greater
Affected Products	Apache Struts 2.0.0 - 2.5.25
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://cwiki.apache.org/confluence/display/WW/S2-061

Affected Product	OpenSSL
Severity	**High**
Affected Vulnerability	Denial of service (CVE-2020-1971)
Description	A vulnerability was identified in OpenSSL. A remote attacker able to control the arguments of the GENERAL_NAME_cmp function, could cause the application, compiled with OpenSSL to crash resulting in which could be exploited by attackers to trigger a denial of service on the targeted system.
Affected Products	OpenSSL Version 1.0.2 and 1.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20201208.txt

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.