Advisory Alert

Alert Number: AAA20210811 **Date:** August 11, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
SonicWall	**Critical**	Remote Code Execution

Description

Affected Product	Microsoft
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26428, CVE-2021-26429, CVE-2021-26430, CVE-2021-26433, CVE-2021-34478, CVE-2021-34485, CVE-2021-34532, CVE-2021-36926, CVE-2021-36932, CVE-2021-36933, CVE-2021-36938, CVE-2021-36941, CVE-2021-36949)
Description	Microsoft has released security updates addressing multiple vulnerabilities that exists in their products. The most severe could cause privilege escalation, remote code execution, memory corruption vulnerability, denial of service and information disclosure. Microsoft highly recommends to apply necessary security fixes to avoid issues.
Affected Products	.NET Core & Visual Studio ASP .NET Azure Azure Sphere Microsoft Azure Active Directory Connect Microsoft Dynamics Microsoft Graphics Component Microsoft Office Microsoft Office SharePoint Microsoft Office Word Microsoft Scripting Engine Microsoft Windows Codecs Library Remote Desktop Client Windows Bluetooth Service Windows Cryptographic Services Windows Defender Windows Event Tracing Windows Media Windows MSHTML Platform Windows NTLM Windows Print Spooler Components Windows Services for NFS ONCRPC XDR Driver Windows Storage Spaces Controller Windows TCP/IP Windows Update Windows Update Assistant Windows User Profile Service
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-Aug

Affected Product	SoniWall
Severity	**Critical**
Affected Vulnerability	Remote Code Execution (CVE-2021-20032)
Description	SonicWall has released security updates addressing remote code execution vulnerability that exists in their product. SonicWall Analytics On-Prem contain a critical Java Debug Wire Protocol (JWDP) service vulnerability that potentially can be leveraged by a remote, unprivileged user to execute arbitrary code within the system. SonicWall highly recommends to apply necessary security fixes to avoid issues.
Affected Products	Analytics On-Prem 2.5.2518 and earlier.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0018

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.