Advisory Alert

Alert Number: AAA20220816 **Date:** August 16, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**	
Severity	**High**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-35822, CVE-2022-34711)	
Description	Microsoft has released security updates addressing multiple vulnerabilities that exist in multiple products. **CVE-2022-35822**- A Security Bypass Vulnerability exists due to unspecified error in Windows Defender Credential Guard. The vulnerability allows a local user to bypass Kerberos protection. **CVE-2022-34711**- A Buffer Overflow Vulnerability exists due to a boundary error in Windows Defender Credential Guard. A local user can trigger memory corruption and execute arbitrary code with SYSTEM privileges. Microsoft highly recommends to apply necessary security fixes at earliest to avoid issues	
Affected Products	Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 for ARM64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems	Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35822 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34711	

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.