Advisory Alert

Alert Number: AAA20220914 **Date:** September 14, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Vulnerabilities
Redhat	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**	
Severity	**High**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23960, CVE-2022-26928, CVE-2022-26929, CVE-2022-30170, CVE-2022-30196, CVE-2022-30200, CVE-2022-3038, CVE-2022-3039, CVE-2022-3040, CVE-2022-3041, CVE-2022-3044, CVE-2022-3045, CVE-2022-3046, CVE-2022-3047, CVE-2022-3053, CVE-2022-3054, CVE-2022-3055, CVE-2022-3056, CVE-2022-3057, CVE-2022-3058, CVE-2022-3075, CVE-2022-33647, CVE-2022-33679, CVE-2022-34700, CVE-2022-34718,CVE-2022-34719, CVE-2022-34721, CVE-2022-34722, CVE-2022-34723, CVE-2022-34725, CVE-2022 34726, CVE-2022-34727, CVE-2022-34728, CVE-2022-34729, CVE-2022-34730, CVE-2022-34731, CVE-2022-34732, CVE-2022-34733, CVE-2022-34734, CVE-2022-35803, CVE-2022-35805, CVE-2022-35823, CVE-2022-35828, CVE-2022-35830, CVE-2022-35831, CVE-2022-35834, CVE-2022-35835, CVE-2022-35836, CVE-2022-35837, CVE-2022-35840, CVE-2022-35841, CVE-2022-37954, CVE-2022-37955, CVE-2022-37956, CVE-2022-37957, CVE-2022-37958, CVE-2022-37959, CVE-2022-37961, CVE-2022-37962, CVE-2022-37963, CVE-2022-37969, CVE-2022-38004, CVE-2022-38005, CVE-2022-38006, CVE-2022-38007, CVE-2022-38008, CVE-2022-38009, CVE-2022-38010, CVE-2022-38011, CVE-2022-38012, CVE-2022-38019, CVE-2022-38020)	
Description	Microsoft has released its September 2022 Security Updates to address multiple vulnerabilities across several 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	.NET and Visual Studio .NET Framework Azure Arc Cache Speculation HTTP.sys Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Office Microsoft Office SharePoint Microsoft Office Visio Microsoft Windows ALPC Microsoft Windows Codecs Library Network Device Enrollment Service (NDES) Role: DNS Server Role: Windows Fax Service SPNEGO Extended Negotiation Visual Studio Code Windows Common Log File System Driver	Windows Credential Roaming Service Windows Defender Windows Distributed File System (DFS) Windows DPAPI (Data Protection Application Programming Interface) Windows Enterprise App Management Windows Event Tracing Windows Group Policy Windows IKE Extension Windows Kerberos Windows Kernel Windows LDAP - Lightweight Directory Access Protocol Windows ODBC Driver Windows OLE Windows Photo Import API Windows Print Spooler Components Windows Remote Access Connection Manager Windows Remote Procedure Call Windows TCP/IP Windows Transport Security Layer (TLS)
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep	

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21123, CVE-2022-21125, CVE-2022-21166, CVE-2022-1729)
Description	Red Hat has released Security Updates addressing multiple kernel updates that exist there Red Hat Linux kernel. Exploitation of these vulnerabilities could cause information disclosure via local access, Privilege Escalation or crash the system. RedHat recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux Server - TUS 7.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:6437 https://access.redhat.com/errata/RHSA-2022:6432

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.