Advisory Alert

Alert Number: AAA20220531 **Date:** May 31, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
Microsoft	**High**	Remote Execution Vulnerability

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-24903, CVE-2022-1552)
Description	Redhat has released updates to address a flaw which was found in PostgreSQL & Rsyslog **CVE-2022-24903**- Due to a flow in rsyslog's reception TCP modules, an attacker could craft a malicious message leading to a heap-based buffer overflow. This further allows the attacker to corrupt or access data stored in memory, leading to a denial of service in the rsyslog or possible remote code execution. **CVE-2022-1552**- Redhat has released updates to address a flaw which was found in PostgreSQL due to incomplete efforts to operate safely when a privileged user is maintaining another user's objects. The Autovacuum, REINDEX, CREATE INDEX, REFRESH MATERIALIZED VIEW, CLUSTER, and pg_amcheck commands activated relevant protections too late or not at all during the process. This flaw allows an attacker with permission to create non-temporary objects in at least one schema to execute arbitrary SQL functions under a superuser identity. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux 6, 7, 8, 9 Red Hat Virtualization 4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2022-1552 https://access.redhat.com/security/cve/CVE-2022-24903

Affected Product	**Microsoft**	
Severity	**High**	
Affected Vulnerability	Remote Execution Vulnerability (CVE-2022-30190)	
Description	Microsoft has released security update to address a remote code execution vulnerability that exists when MSDT is called using the URL protocol from a calling application such as Word. Successful exploitation of this flaw leads an attacker to run arbitrary code with the privileges of the calling application and install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights. Microsoft highly recommends to apply necessary security fixes at earliest to avoid issues	
Affected Products	Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64based Systems-Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64based Systems-Service Pack 1 Windows Server 2008 for x64based Systems-Service Pack 2 (Server Core installation) Windows Server 2008 for x64based Systems-Service Pack 2 Windows Server 2008 for 32bit Systems Service-Pack 2 (Server Core installation) Windows Server 2008 for 32bit Systems Service - Pack 2 Windows RT 8.1 Windows 8.1 for x64based systems Windows 8.1 for 32bit systems Windows 7 for x64based Systems Service Pack 1 Windows 7 for 32bit Systems Service Pack 1 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64based Systems Windows 10 Version 1607 for 32bit Systems Windows 10 for x64based Systems Windows 10 for 32bit Systems Windows 10 Version 21H2 for x64based Systems	Windows 10 Version 21H2 for ARM64based-Systems Windows 10 Version 21H2 for 32bit Systems Windows 11 for ARM64based Systems Windows 11 for x64based Systems Windows Server, version 20H2 (Server Core-Installation) Windows 10 Version 20H2 for ARM64based-Systems Windows 10 Version 20H2 for 32bit Systems Windows 10 Version 20H2 for x64based Systems Windows Server 2022 Azure Edition Core Hotpatch Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for 32bit Systems Windows 10 Version 21H1 for ARM64based-Systems Windows 10 Version 21H1 for x64based Systems Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64based-Systems Windows 10 Version 1809 for x64based Systems Windows 10 Version 1809 for 32bit Systems
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190	

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.