secpod

SECPOD'S REPORT ON PATCH TUESDAY UPDATES - Q1 2021

A summary of high-risk vulnerabilities you need to patch in Microsoft applications this quarter

www.secpod.com

Table of **Contents**

Patch Tuesday is the most important day of the month for security teams. Microsoft releases patches for vulnerabilities discovered in the previous month all at once in the second Tuesday of every month calling it “Patch Tuesday”. The severity of the vulnerabilities are classified as: **Critical, Important, Moderate**, and **Low** based on their risk levels.

How to use this document

Microsoft releases patches for hundreds of vulnerabilities on a single day, which makes it difficult to prioritize the patches and fix the vulnerabilities that pose the most risk. To make your patching efforts easy, we have listed and categorized all vulnerabilities of 2021 Q1’s Patch Tuesday updates

- Share this document with all members of your patching team
- Prioritize and patch the vulnerabilities in the ‘Critical’ list included in this document
- Use it as a centralized source of information for your team to verify completed updates or clear the backlog of Patch Tuesday updates from January to March 2021

Deployed all the patches already? It never hurts to cross-check again.

Patch Tuesday January 2021

Microsoft rolled out its January Patch Tuesday **security updates** for 83 vulnerabilities, including a zero-day. The updates covered products such as Windows OS, Edge browser, Microsoft Office and services, and developer tools.

Patch Tuesday January 2021	
Critical	10
Important	73
Total number of vulnerabilities	**83**

January's most Critical vulnerabilities that require immediate patching

Microsoft Defender remote code execution vulnerability | CVE-2021-1647

CVSS score: 7.8 (High)

Affected product: Microsoft Malware Protection Engine

About the vulnerability

This zero-day in Windows Defender affects Microsoft Windows running Microsoft Malware Protection Engine. According to CVSS, this actively exploited vulnerability takes a high impact (critical) when the attacker exploits it against the unpatched systems. The users can be tricked into opening a malicious document sent by the attackers targeting the unpatched systems, which leads to remote code execution. This active exploit is already disclosed and has proof of concept, making the probability even high to perform a successful attack against an unpatched system.

Impact:

On successful exploitation, the malicious actor can acquire the admin-level privileges, which could lead to a full system compromise, including view, modify, delete the local data. While exploited against admin mode, the attacker can create new users and would be able to modify existing user privileges.

Remote Procedure Call Runtime remote code execution vulnerability | CVE-2021-1660

CVSS score: 8.8 (High)

Affected product: Microsoft Windows

About the vulnerability

Microsoft Windows could allow a remote authenticated attacker to execute arbitrary code on the system, caused by a flaw in the Remote Procedure Call Runtime. More technical details of the exploit are not available.

Impact:

By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system with privileges of the victim.

Multiple vulnerabilities in Microsoft HEVC Video Extensions | CVE-2021-1643, CVE-2021-1644

CVSS score: 7.8 (High), 7.8 (High)

Affected product: Microsoft Windows Codecs Library

About the vulnerability

The vulnerabilities exist due to insufficient validation of user-supplied input in HEVC Video Extensions. More technical details of the exploit are not available.

Impact:

A remote attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

List of all Critical vulnerabilities in January

Product	CVEs/Advisory	Impact	KBs	Severity
Microsoft Windows	CVE-2021-1637, CVE-2021-1638, CVE-2021-1642, CVE-2021-1645, CVE-2021-1646, CVE-2021-1648, CVE-2021-1649, CVE-2021-1650, CVE-2021-1651, CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1656, CVE-2021-1657, CVE-2021-1658, CVE-2021-1659, CVE-2021-1660, CVE-2021-1661, CVE-2021-1662, CVE-2021-1663, CVE-2021-1664, CVE-2021-1665, CVE-2021-1666, CVE-2021-1667, CVE-2021-1668, CVE-2021-1669, CVE-2021-1670,	Elevation of Privilege, Remote Code Execution, Information Disclosure, Denial of Service,	4598229, 4598230, 4598231, 4598242, 4598243, 4598245, 4598275, 4598278,	Critical

Product	CVEs/Advisory	Impact	KBs	Severity
	CVE-2021-1637, CVE-2021-1638, CVE-2021-1642, CVE-2021-1645, CVE-2021-1646, CVE-2021-1648, CVE-2021-1649, CVE-2021-1650, CVE-2021-1651, CVE-2021-1652, CVE-2021-1653, CVE-2021-1654, CVE-2021-1655, CVE-2021-1656, CVE-2021-1657, CVE-2021-1658, CVE-2021-1659, CVE-2021-1660, CVE-2021-1661, CVE-2021-1662, CVE-2021-1663, CVE-2021-1664, CVE-2021-1665, CVE-2021-1666, CVE-2021-1667, CVE-2021-1668, CVE-2021-1669, CVE-2021-1670, CVE-2021-1671, CVE-2021-1672, CVE-2021-1673, CVE-2021-1674, CVE-2021-1676, CVE-2021-1678, CVE-2021-1679, CVE-2021-1680, CVE-2021-1681, CVE-2021-1682, CVE-2021-1683, CVE-2021-1684, CVE-2021-1685, CVE-2021-1686, CVE-2021-1687, CVE-2021-1688, CVE-2021-1689, CVE-2021-1690, CVE-2021-1691, CVE-2021-1692, CVE-2021-1693, CVE-2021-1694, CVE-2021-1695, CVE-2021-1696, CVE-2021-1697, CVE-2021-1699, CVE-2021-1700, CVE-2021-1701, CVE-2021-1702, CVE-2021-1703, CVE-2021-1704, CVE-2021-1706, CVE-2021-1708, CVE-2021-1709, CVE-2021-1710	Security Feature Bypass, Spoofing	4598285, 4598297	
Microsoft Edge (EdgeHTML-based)	CVE-2021-1705	Remote Code Execution	4598229, 4598230, 4598231, 4598242, 4598243, 4598245	Critical
Microsoft Windows Codecs Library	CVE-2021-1643, CVE-2021-1644	Remote Code Execution		Critical
Microsoft Malware Protection Engine	CVE-2021-1647	Remote Code Execution		Critical

List of all Important vulnerabilities in January

Product	CVEs/Advisory	Impact	KBs	Severity
Microsoft Office and Microsoft Office Services and Web Apps	CVE-2021-1641, CVE-2021-1707, CVE-2021-1711, CVE-2021-1712, CVE-2021-1713, CVE-2021-1714, CVE-2021-1715, CVE-2021-1716, CVE-2021-1717, CVE-2021-1718, CVE-2021-1719	Elevation of Privilege, Remote Code Execution, Spoofing, Tampering	4486683, 4486724, 4486736, 4486755, 4486759, 4486762, 4486764, 4493142, 4493143, 4493145, 4493156, 4493160, 4493161, 4493162, 4493163, 4493165, 4493167, 4493168, 4493171, 4493175, 4493176, 4493178, 4493181, 4493183, 4493186, 4493187	Important
Developer Tools (Visual Studio, .NET Core, .NET	CVE-2020-26870, CVE-2021-1651, CVE-2021-1680,	Elevation of Privilege, Remote Code Execution,	4584787	Important
Framework, SDK (Python, JS, .NET Framework)	CVE-2021-1723, CVE-2021-1725	Information Disclosure, Denial of Service		
SQL Server	CVE-2021-1636	Elevation of Privilege	4583456, 4583457, 4583458, 4583459, 4583460, 4583461, 4583462, 4583463, 4583465	Important
SQL Server	CVE-2021-1636	Elevation of Privilege	4583456, 4583457, 4583458, 4583459, 4583460, 4583461, 4583462, 4583463, 4583465	Important
Azure	CVE-2021-1677	Spoofing		Important

Patch Tuesday February 2021

Microsoft rolled-out its February Patch Tuesday **security updates** for 56 vulnerabilities, including a zero-day. The updates covered products such as Windows OS, Edge browser, Microsoft Office, and services.

Patch Tuesday February 2021	
Critical	11
Important	43
Moderate	2
Total number of vulnerabilities	**56**

February's most Critical vulnerabilities that require immediate patching

Windows Win32k elevation of privilege vulnerability | CVE-2021-1732

CVSS score: 7.8 (High)

Affected product: Microsoft Windows

About the vulnerability

This zero-day affects Windows 10, Server 2016, and later editions of Windows OS. According to CVSS, this actively exploited vulnerability takes an impact level of 'Important'. The affected modules cannot be overlooked even though the severity is non-critical. Win32k.sys is a common system file used by the Windows kernel, mostly targeted by evasive malware. This particular vulnerability exposure requires an authenticated attacker to succeed. Hence it is important and non-critical. But unauthenticated attackers can target an existing vulnerability in the affected system to exploit Win32k. This is a highly expected exploitation technique, a known issue from the past.

Impact:

On successful exploitation, an attacker can gain system-level access by elevating their privilege to administrative privileges.

Windows DNS Server remote code execution vulnerability | CVE-2021-24078

CVSS score: 9.8

Affected product: Microsoft Windows, Windows Server

About the vulnerability

This is a bug in the Windows DNS Server that could allow remote code execution on affected systems. Fortunately, if the system is not configured to be a DNS server, it is not impacted by this bug. However, for those systems that are configured as DNS servers, this bug allows code execution in a privileged service from a remote, unauthenticated attacker.

Impact:

On successful exploitation, an attacker can execute code remotely. This is potentially wormable, although only between DNS servers.

Multiple vulnerabilities affecting TCP/IP | CVE-2021-24074, CVE-2021-24094

CVSS score: 9.8 (Critical), 9.8 (Critical)

Affected product: Microsoft Windows, Windows Server

About the vulnerability

Technical details for the exploit were not released, but both vulnerabilities can cause remote code execution.

Impact:

An attacker who successfully exploits these vulnerabilities may be able to execute arbitrary code on the target system.

List of all Critical vulnerabilities in February

Product	CVEs/Advisory	Impact	KBs	Severity
Microsoft Windows (Address Book, Backup Engine, Console Driver, Defender, DirectX, Event Tracing, Installer, Mobile Device Management,- Network File System, PFX Encryption, PKU2U, PowerShell, Print Spooler Components, Remote Procedure Call, TCP/IP, Trust Verification API, Windows Codecs Library, Microsoft Graphics Component)	CVE-2020-17162, CVE-2021-1698, CVE-2021-1722, CVE-2021-1727, CVE-2021-1731, CVE-2021-1732, CVE-2021-1734, CVE-2021-24074, CVE-2021-24075,CVE-2021-24076, CVE-2021-24077,CVE-2021-24078, CVE-2021-24079,CVE-2021-24080, CVE-2021-24081,CVE-2021-24082, CVE-2021-24083,CVE-2021-24084, CVE-2021-24086,CVE-2021-24088, CVE-2021-24091,CVE-2021-24093, CVE-2021-24094,CVE-2021-24096, CVE-2021-24098,CVE-2021-24102, CVE-2021-24103,CVE-2021-24106, CVE-2021-25195	Denial of Service, Elevation of Privilege, Information Disclosure, Remote Code Execution, Security,Feature Bypass	4570333, 4571756, 4574727, 4577015, 4577032, 4577038, 4577048, 4577049, 4577066, 4577071, 4601315, 4601318, 4601319, 4601331, 4601345, 4601348, 4601349, 4601354, 4601357, 4601384	Critical
Developer Tools (.NET Core, .NET Framework, Visual Studio, Visual Studio Code)	CVE-2021-1639, CVE-2021-1721, CVE-2021-24105, CVE-2021-24111, CVE-2021-24112, CVE-2021-26700, CVE-2021-26701	Denial of Service, Elevation of Privilege, Remote Code Execution	4601050, 4601051, 4601054, 4601056, 4601318, 4601354, 4601887, 4602958, 4602959, 4602960, 4602961, 4603002, 4603003, 4603004, 4603005	Critical
Sysinternals	CVE-2021-1733	Elevation Of Privilege		Critical
Microsoft Exchange Server	CVE-2021-1730, CVE-2021-24085	Spoofing	4602269, 4571788	Critical

List of all Important vulnerabilities in February

Product	CVEs/Advisory	Impact	KBs	Severity
Microsoft Office (Lync, Office, Teams, Skype, SharePoint)	CVE-2021-1726, CVE-2021-24066, CVE-2021-24067, CVE-2021-24068, CVE-2021-24069, CVE-2021-24070, CVE-2021-24071, CVE-2021-24072, CVE-2021-24073, CVE-2021-24099, CVE-2021-24114	Denial of Service, Impact, Information Disclosure, Remote Code Execution, Spoofing	4493192, 4493194, 4493195, 4493196, 4493204, 4493210, 4493211, 4493222, 4493223, 5000675, 5000688	Important
Azure (IoT, Kubernetes Service)	CVE-2021-24087, CVE-2021-24109	Elevation of Privilege	4601050, 4601051, 4601054, 4601056, 4601318, 4601354, 4601887, 4602958, 4602959, 4602960, 4602961, 4603002, 4603003, 4603004, 4603005	Important
Azure (IoT, Kubernetes Service)	CVE-2021-24087, CVE-2021-24109	Elevation of Privilege		Important
Microsoft Edge for Android	CVE-2021-24100	Information Disclosure		Important
System Center	CVE-2021-1728	Elevation of Privilege	4601269	Important
Microsoft Dynamics	CVE-2021-1724, CVE-2021-24101	Information Disclosure, Spoofing	4595460, 4595463, 4602915	Important

Patch Tuesday March 2021

Microsoft rolled out its March Patch Tuesday **security updates** for 82 vulnerabilities. The updates covered products such as Windows OS, Exchange Server, Office, and other products.

Patch Tuesday March 2021	
Critical	10
Important	72
Total number of vulnerabilities	**82**

March's most Critical vulnerabilities that require immediate patching

Exchange Server vulnerabilities | CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065

CVSS score: 9.8 (Critical), 7.8 (High), 7.8 (High), 7.8 (High)

Affected product: Microsoft Exchange Server 2010, 2013, 2016, 2019

About the vulnerability

All four are zero-day vulnerabilities in Microsoft Exchange Servers. CVE-2021-26855 is a server-side request forgery flaw that allows attackers to send arbitrary hypertext transfer protocol requests from untrusted sources to port 443, and authenticate as the target Exchange Server. Microsoft reported malware spread and data theft attacks on organizations unpatched on-premise Exchange Servers by Hafnium, a hacking group.

Impact

An attacker could send arbitrary HTTP requests and authenticate as the Exchange Server. After authentication, the attacker could either compromise a legitimate admin's credentials or take advantage of other Exchange Server vulnerabilities to execute remote code using Web Shell or steal information about the organization and its users.

Memory corruption vulnerability in Internet Explorer | CVE-2021-26411

CVSS score: 8.8 (High)

Affected product: Microsoft Edge and Internet Explorer 11

About the vulnerability

An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability.

Impact:

An attacker could host the exploit code on a malicious website and convince a user through social engineering tactics to visit the page, or the attacker could inject the malicious payload into a legitimate website, causing memory corruption.

Windows DNS Server remote code execution vulnerability | CVE-2021-26897

CVSS score: 9.8 (Critical)

Affected product: Microsoft Windows DNS Server

About the vulnerability

The vulnerability is triggered when many consecutive Signature RRs Dynamic Updates are sent. This vulnerability impacts any DNS server. The surrounding configuration can limit possible vectors/sources for the attack, but proper mitigation requires the latest patch from March's Patch Tuesday.

Impact:

The exploitation doesn't require any form of authentication and can cause remote code execution

Product	CVEs/Advisory	Impact	KBs	Severity
	CVE-2020-27844, CVE-2021-21149, CVE-2021-21150, CVE-2021-21151, CVE-2021-21152, CVE-2021-21153, CVE-2021-21154, CVE-2021-21155, CVE-2021-21156, CVE-2021-21157, CVE-2021-21159, CVE-2021-21160, CVE-2021-21161, CVE-2021-21162, CVE-2021-21163, CVE-2021-21164, CVE-2021-21165, CVE-2021-21166, CVE-2021-21167, CVE-2021-21168, CVE-2021-21169, CVE-2021-21170, CVE-2021-21171, CVE-2021-21172, CVE-2021-21173, CVE-2021-21174, CVE-2021-21175, CVE-2021-21176, CVE-2021-21177, CVE-2021-21178 , CVE-2021-21179, CVE-2021-21180, CVE-2021-21181, CVE-2021-21182, CVE-2021-21183, CVE-2021-21184, CVE-2021-21185, CVE-2021-21186, CVE-2021-21187, CVE-2021-21188, CVE-2021-21189, CVE-2021-21190			
Microsoft Office	CVE-2021-24104, CVE-2021-24108, CVE-2021-27052, CVE-2021-27053, CVE-2021-27054, CVE-2021-27056, CVE-2021-27057, CVE-2021-27058, CVE-2021-27059, CVE-2021-27076	Remote Code Execution, Information Disclosure, Denial of Service, Spoofing, Tampering	3101541, 4493177, 4493199, 4493200, 4493203, 4493214, 4493224, 4493225, 4493227, 4493228, 4493229, 4493230, 4493231, 4493232, 4493233, 4493234, 4493238, 4493239, 4504702, 4504703, 4504707	Critical
Visual Studio	CVE-2021-21300	Remote Code Execution, Information Disclosure, Denial of Service, Spoofing, Tampering		Critical

List of all Important vulnerabilities in March

Product	CVEs/Advisory	Impact	KBs	Severity
Visual Studio Code	CVE-2021-27081, CVE-2021-27082, CVE-2021-27083, CVE-2021-27084, CVE-2021-27060	Remote Code Execution, Information Disclosure, Denial of Service, Spoofing, Tampering	4598285, 4598297	Important

Deploy patches at scale effortlessly with SanerNow

During monthly routines like Patch Tuesday or any other bulk updates, your security team needs to operate with the best efficiency and collaboration. To keep all data, patching controls, and admins at one place means having good collaboration and efficient operation.

SanerNow Patch Management is a cloud-based tool to help ease your patching process.

- Get the latest patches from vendors ready to deploy in under 24 hours of release
- Automate end-to-end tasks of patching and remediate vulnerabilities with zero manual work
- Role-based access control with individual user logins for better planning and delegation among security teams
- Accurate patch prioritization to help you make faster and better decisions in your patching routines
- Rollback faulty patches to the last stable version and restore uptime immediately

Take 30-Day Free Trial

HEAD OFFICE:
SecPod Technologies Pvt. Ltd. 1354, 9th Cross, 33rd Main, JP Nagar I Phase
Bangalore – 560078, Karnataka, India
Email: info@secpod.com, Phone: (+91) 80 4121 4020