KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft Patch Tuesday Nov 2022

Tracker ID: TN1112 **Date:** 11/Nov/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Microsoft has released Patch Tuesday for November 2022, which includes fixes for 68 vulnerabilities as well as six actively exploited zero-day vulnerabilities. This update addresses CVE-2022-41040 and CVE-2022-41082, also known as "ProxyNotShell" vulnerabilities, affecting Microsoft Exchange Servers. Microsoft also patched 11 critical bugs, 6 actively exploited zero-day vulnerabilities (including PoxyNotShell), and Mark of the Web (MotW) security flaws. It addressed 27 privilege escalations, four security feature bypass, sixteen remote code executions, eleven information disclosures, six denial of service (DoS) vulnerabilities, and three spoofing vulnerabilities.

Below six zero-days were patched:

CVE-2022-41040 and CVE-2022-41082 : CVE-2022-41040 is a Microsoft Exchange Server elevation of privilege bug that could allow an attacker to run PowerShell in the context of the system, whereas CVE-2022-41082 is a Microsoft Exchange Server remote code execution flaw that could allow an attacker to perform arbitrary or remote code execution on the MS server accounts. Both of these flaws are referred to as "ProxyNotShell.“

CVE-2022-41128 : A vulnerability in Windows scripting languages that allows remote code execution. To exploit this issue, a threat actor must deceive a victim running a vulnerable version of Windows into connecting to a malicious server where an attacker has pre-hosted a specially crafted server share or website.

CVE-2022-41073 and CVE-2022-41125 : CVE-2022-41073 and CVE-2022-41125 are both elevation of privilege flaws. CVE-2022-41073 is a privilege escalation vulnerability in Windows Print Spooler, whereas CVE-2022-41125 is a privilege escalation vulnerability in Windows CNG Key Isolation Service. An attacker could acquire SYSTEM privileges if these vulnerabilities are successfully exploited.

CVE-2022-41091 : It is a Windows Mark of the Web Security Feature Bypass Vulnerability in which a malicious file created by an attacker could circumvent Mark of the Web (MOTW) protections, resulting in a loss of integrity and availability of security features that rely on MOTW tagging, such as Protected View in Microsoft Office.

These fixes addressed critical vulnerabilities (CVEs) affecting the full range of the security product line, including Azure, BitLocker, Dynamics, Exchange Server, Office, and Office components, Network Policy Server (NPS), SharePoint Server, SysInternals, Visual Studio, Windows, and Windows components, as well as Linux kernel and other open-source software bugs that affect Microsoft products.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft Patch Tuesday Nov 2022

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-41082	High	8.8
CVE-2022-41040	High	8.8
CVE-2022-41128	High	8.8
CVE-2022-41073	High	7.8
CVE-2022-41125	High	7.8
CVE-2022-41091	Medium	5.4

Affected Products and Versions

- CVE-2022-41082 & CVE-2022-41040 affects : Microsoft Exchange Server 2013, 2016 and 2019.
- CVE-2022-41128 affects: Windows 7, 8 and 10 versions and Windows Servers 2008, 2012, 2016, and 2019.
- CVE-2022-41125 affects: Windows 8, 10, and 11 versions and Windows Servers 2012, 2016, 2019, 20H2 and 21H2.
- CVE-2022-41073 affects : Windows 7, 8, 10 and 11 versions and Windows Servers 2008, 2012, 2016, and 2019.
- CVE-2022-41091 affects: Windows 10 and 11 versions and Windows Servers 2019, 2022, 20H2, 21H2 and 2016.

Recommendations

- Administrators and organizations are encouraged to identify the vulnerable instances and implement the vendor-provided patch as soon as possible.

References

- Security Update Guide: Please apply filter for November, Microsoft, 08th November 2022, External Link (msrc.microsoft.com)
- Patch Tuesday, November 2022 Election Edition, Kebros on Security, 08th November 2022, External Link (krebsonsecurity.com)
- Lawrence Abrams, Microsoft November 2022 Patch Tuesday fixes 6 exploited zero-days, 68 flaws, Bleeping Computer, 08th November 2022, External Link (bleepingcomputer.com)
- Renato Marinho, Microsoft November 2022 Patch Tuesday, SANS, 08th November 2022, External Link (isc.sans.edu)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft Patch Tuesday Nov 2022

In case of a Security Incident, please report to IN-FM KPMG SOC.
For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia