KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Critical Remote Code Execution in Microsoft Key Exchange exploited

Tracker ID: TN1201 **Date:** 01/Dec/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

CVE-2022-34721, a critical vulnerability affecting Microsoft Windows IKE Protocol Extensions, has been identified and is being actively exploited. The campaign, which translates as "bleed you," could have targeted over 1,000 systems. Recently, unidentified hackers posted a link to a vulnerability on darknet forums that could be used to infiltrate vulnerable systems. The campaign takes advantage of the recently discovered flaw to steal sensitive data for monetary gain, get elevated access, and disrupt operations.

The campaign is aimed at multiline retail, industrial conglomerates, governments, financial services, information technology, and commercial services. The countries targeted are the United States, the United Kingdom, Australia, India, Canada, France, Japan, Germany, and Turkey.

The vulnerability is identified in the code that handles the deprecated IKEv1 (Internet Key Exchange) protocol, which is still compatible with legacy systems. An unauthenticated attacker could send a specially crafted IP packet to a target machine running Windows with IPSec enabled, allowing remote code execution. This issue is fixed by putting a check on the length of incoming data and skipping processing if it is too short.

The exploit takes advantage of memory corruption in the svchost process of the vulnerable machine. When the system's Page Heap (a debugging plug-in) for the Internet Key Exchange process is enabled, memory corruption occurs, and when attempting to read data past an allotted buffer, the exe process hosting the Internet Key Exchange protocol service crashes. This issue affects only IKEv1; IKEv2 is unaffected. However, because they receive both V1 and V2 packets, all Windows servers are impacted.

Researchers have found unknown Chinese threat actors collaborating with Russian hackers (FIN7) to potentially exploit this vulnerability to carry out their nefarious activities. The "bleed you" campaign shows a possible strategic relationship between Russia and China based on changing geopolitical conditions and external threat landscape management.

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-34721	Critical	9.8

Affected Products and Versions

- Windows 7, 8.1, 11 and 10 20H2, 21H1, 21H2 and 1809 versions.
- Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 and 2022.

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

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Critical Remote Code Execution in Microsoft Key Exchange exploited

Tracker ID: TN1201 **Date:** 01/Dec/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Recommendations

- Check whether the vulnerable IKE and AuthIP IPsec Keying Modules is running on the systems using the following command:
  - On PS: C:\&gt; Get-Service Ikeext OR On Cmd: C:\&gt; sc query ikeext
- Immediately identify the vulnerable instances and apply the latest patch update.

References

- Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability, Microsoft, 23rd November 2022, External Link (msrc.microsoft.com)
- Windows Internet Key Exchange (IKE) Remote Code Execution Vulnerability Analysis, Cyfirma, 23rd November 2022, External Link (cyfirma.com)
- CVE-2022-34721 Detail, Microsoft, 15th November 2022, External Link (nvd.nist.gov)

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