GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

19 August 2026

Advisory 190: CVE-2026-33824_Microsoft Internet Key Exchange (IKE) Service Extensions Double Free Vulnerability

Release Date: 14th April 2026 (Added 18 August 2026)
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-33824 is a critical-severity remote code execution vulnerability in the Windows Internet Key Exchange (IKE) Extension, the service that negotiates and manages secure tunnels for VPNs and other IPsec-based connections. It carries a CVSS Base Score of 9.8 and is caused by a double-free memory corruption condition (CWE-415) triggered while processing IKEv2 packet fragments. An unauthenticated, remote attacker can send specially crafted packets to a Windows host with IKEv2 enabled to trigger the flaw, with no user interaction required. The Zero Day Initiative rated this among its "bugs of the month" for April 2026 and flagged it as wormable, alongside a separate Windows TCP/IP vulnerability patched in the same release. Microsoft fixed CVE-2026-33824 in the 14 April 2026 Patch Tuesday release.

What are the systems affected?

Affected systems include any Windows client or server with IKEv2 enabled - for example, for site-to-site VPNs, remote access VPNs, or Windows Always on VPN - since the IKE Extension is necessarily reachable from untrusted networks to perform its function.

Windows 10 (supported versions) – (Affected)
Windows 11 (all supported versions) – (Affected)
Windows Server 2016 – (Affected, fixed in 10.0.14393.9060)
Windows Server 2019 – (Affected, fixed in 10.0.17763.8644)
Windows Server 2022 – (Affected, fixed in 10.0.20348.5020)
Windows Server 2025 – (Affected, fixed in 10.0.26200.8246)
Windows hosts without IKEv2/IPsec enabled – (Not exposed to this vector)

Any organisation running internet-facing VPN gateways or DirectAccess servers with IKEv2 should treat patching as urgent, since these are reachable in a pre-authentication context by design.

What does this mean?

This flaw sits at the network perimeter by design: IKE must be reachable from untrusted networks to negotiate VPN tunnels, so there is no initial-access step for the attacker to complete first - reachability is the only prerequisite.

Step 1 - Crafted Packet Delivery
The attacker sends specially crafted IKEv2 packets to UDP port 500 or 4500 on a target Windows host with IKE enabled. No credentials, prior access, or user interaction are required.

Step 2 - Fragment Processing Error
The malformed fragments trigger an error in how the IKE Extension (ikeext.dll) reassembles and frees memory, causing the same memory address to be freed twice.

Step 3 - Memory Corruption
This double-free condition corrupts heap memory in a way that can be shaped by the attacker, turning a memory-safety bug into a controllable primitive for hijacking program execution.

Step 4 - SYSTEM-Level Code Execution
A successful exploit gives the attacker **arbitrary code execution at SYSTEM level** on the affected host - full compromise of a VPN gateway or any other IKE-enabled machine, reachable from an untrusted network with no authentication.

Mitigation process

CERTVU recommends the following:

1. **Apply the April 2026 Security Update**

Confirm the 14 April 2026 Patch Tuesday cumulative update, or a later cumulative update that supersedes it, is installed on every Windows client and server, prioritizing internet-facing VPN

gateways and DirectAccess servers first. Fixed builds include 10.0.14393.9060 (Server 2016), 10.0.17763.8644 (Server 2019), 10.0.20348.5020 (Server 2022), and 10.0.26200.8246 (Windows 11 25H2 / Server 2025), among others.

Microsoft Security Update Guide: CVE-2026-33824

2. Compensating Controls Where Patching Is Delayed

For any system that cannot be patched immediately, block inbound UDP ports 500 and 4500 at the network perimeter on hosts that do not require IKE, or restrict inbound traffic on those ports to known peer addresses only where IKE is required. On hosts where IPsec VPN functionality is not in use, disable the IKEEXT service entirely as an additional compensating control.

Note: These measures reduce exposure but do not fully remediate the vulnerability - only the security update does.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-33824
3. https://www.thezdi.com/blog/2026/4/22/cve-2026-33824-remote-code-execution-in-windows-ikev2

.