Microsoft Addresses Actively Exploited Exchange Vulnerability and Multiple Zero-Days

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Microsoft released updates for nearly 200 vulnerabilities. The updates include one actively exploited Microsoft Exchange Server vulnerability (CVE-2026-42897), multiple publicly disclosed zero-days linked to researcher Nightmare Eclipse, and several critical remote code execution vulnerabilities affecting core Windows services.

Overview

Microsoft released security updates for an actively exploited Exchange Server vulnerability (CVE-2026-42897), several publicly disclosed Windows vulnerabilities, and multiple critical flaws affecting Windows networking and authentication components. Some of the patched vulnerabilities are linked to recent disclosures from Nightmare Eclipse, while a new exploit known as RoguePlanet emerged shortly after the updates were released.

Affected Products

Microsoft Exchange Server	Windows HTTP.sys
Microsoft Defender	Windows DHCP Client Service
Microsoft Windows	Windows Kernel
Windows Collaborative Translation Framework (CTFMON)	Microsoft Office
	Microsoft SharePoint
Windows BitLocker	Microsoft Hyper-V
Remote Desktop Client	Active Directory Domain Services

The Vulnerabilities

- Microsoft Exchange Server Cross-Site Scripting Vulnerability (CVE-2026-42897, CVSS 8.1)
  - Microsoft confirmed active exploitation of this vulnerability. An attacker can send a specially crafted email that may execute arbitrary JavaScript when opened through Outlook Web Access (OWA).
- Windows Collaborative Translation Framework Privilege Escalation Vulnerability (CVE-2026-45586, CVSS 7.8)
  - Publicly disclosed by Nightmare Eclipse as "GreenPlasma," this vulnerability allows an authenticated attacker to obtain SYSTEM privileges.

- Windows BitLocker Security Feature Bypass Vulnerability (CVE-2026-45585, CVSS 6.8)
    - Publicly disclosed by Nightmare Eclipse as "YellowKey," this vulnerability may allow an attacker with physical access to bypass BitLocker protections and access encrypted data on affected systems.
- Windows BitLocker Security Feature Bypass Vulnerability (CVE-2026-50507, CVSS 6.8)
    - Another publicly disclosed BitLocker bypass vulnerability that may allow attackers with physical access to access encrypted drives on affected Windows devices.
- HTTP.sys Denial-of-Service Vulnerability (CVE-2026-49160, CVSS 7.5)
    - A publicly disclosed vulnerability affecting Windows systems that process HTTP and HTTPS traffic. Successful exploitation could cause affected systems or services to become unavailable.
- Windows DHCP Client Service Remote Code Execution Vulnerability (CVE-2026-44815, CVSS 9.8)
    - A critical remote code execution vulnerability affecting the Windows DHCP Client Service, which is present on most Windows systems. Successful exploitation could allow remote code execution without user interaction.
- Windows Kernel Remote Code Execution Vulnerability (CVE-2026-45657, CVSS 8.8)
    - This vulnerability affects how Windows processes network traffic and could allow remote code execution on affected systems.

Shortly after Microsoft's security updates were released, Nightmare Eclipse disclosed RoguePlanet, another Windows privilege escalation exploit. Aspire's CTI team recently published an Emergency Flash Notice covering the researcher's GreenPlasma and YellowKey vulnerabilities.

Aspire Protects

- **Microsoft Exchange Server Cross-Site Scripting Vulnerability (CVE-2026-42897)**
    - Install the June 2026 Exchange Server security updates immediately.
    - Verify the Exchange Emergency Mitigation Service (EEMS) remains enabled.
- **Windows Collaborative Translation Framework Privilege Escalation Vulnerability (CVE-2026-45586)**
    - Apply Microsoft's June 2026 Windows security updates.

    - Monitor for unauthorized SYSTEM-level processes and privilege escalation activity.
- **Windows BitLocker Security Feature Bypass Vulnerabilities (CVE-2026-45585, CVE-2026-50507)**
    - Apply Microsoft's security updates.
    - Restrict physical access to affected systems.
- **HTTP.sys Denial-of-Service Vulnerability (CVE-2026-49160)**
    - Apply Microsoft's security update as soon as possible.
    - Implement Microsoft's recommended HTTP.sys mitigations if patching must be delayed.
- **Windows DHCP Client Service Remote Code Execution Vulnerability (CVE-2026-44815) and Windows Kernel Remote Code Execution Vulnerability (CVE-2026-45657)**
    - Prioritize patching affected Windows systems, especially internet-facing and business-critical assets.
- **RoguePlanet**
    - Ensure Microsoft Defender platform and intelligence updates are current.
    - Monitor for suspicious SYSTEM-level process creation originating from Defender-related activity.

TTPs

Initial Access

- Exploit Public-Facing Application [T1190] – Exploitation of Outlook Web Access (OWA) and Exchange Server components (CVE-2026-42897)

Execution

- Command and Scripting Interpreter: JavaScript [T1059.007] – Execution of JavaScript within a victim browser session (CVE-2026-42897)

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – Elevation to SYSTEM privileges through Windows privilege escalation vulnerabilities (CVE-2026-45586)
- Exploitation for Privilege Escalation [T1068] – SYSTEM-level access through a Windows privilege escalation exploit (RoguePlanet)

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations across all sectors that rely on Microsoft technologies may be affected, particularly those operating on-premises Exchange Server environments and Windows-based infrastructure.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2026-42897 - Security Update Guide - Microsoft - Microsoft Exchange Server Spoofing Vulnerability

Will Dormann: "Nightmare Eclipse has released…" - Infosec Exchange

CVE-2026-45586 - Security Update Guide - Microsoft - Windows Collaborative Translation Framework (CTFMON) Elevation of Privilege Vulnerability

CVE-2026-49160 - Security Update Guide - Microsoft - HTTP.sys Denial of Service Vulnerability

CVE-2026-44815 - Security Update Guide - Microsoft - DHCP Client Service Remote Code Execution Vulnerability

CVE-2026-50507 - Security Update Guide - Microsoft - Windows BitLocker Security Feature Bypass Vulnerability

CVE-2026-45585 - Security Update Guide - Microsoft - Windows BitLocker Security Feature Bypass Vulnerability

CVE-2026-45657 - Security Update Guide - Microsoft - Windows Kernel Remote Code Execution Vulnerability

Nightmare Eclipse: Two more public disclosures, it will never stop