APT34 Exploits Windows Vulnerability – CVE-2024-30088

Overview

This week, the Cybersecurity and Infrastructure Security Agency (CISA) added a previously patched Microsoft vulnerability (CVE-2024-30088, CVSS 7) to their Known Exploited Vulnerabilities (KEV) catalog. The Iranian state-backed threat actor APT34, also known as OilRig, has launched new attacks against government and critical infrastructure organizations in the United Arab Emirates and the Gulf region.

These attacks leverage CVE-2024-30088 to elevate privileges on compromised systems. The campaign includes exploitation of on-premise Microsoft Exchange servers and a new backdoor, StealHook, to steal credentials.

CVE-2024-30088 is a high-severity privilege escalation vulnerability in the Windows kernel, first patched by Microsoft in June 2024. Exploitation of this vulnerability allows attackers to elevate their privileges to SYSTEM level, giving them significant control over targeted devices. The flaw involves a race condition (CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition).

Affected Products:

- Microsoft Windows 10 (various versions)
- Microsoft Windows 11 (various versions)
- Windows Server 2016, 2019, 2022

Despite CVE-2024-30088 being added to CISA's KEV catalog and Trend Micro's report acknowledging exploitation of the vulnerability, neither Microsoft nor CISA has marked the vulnerability as being actively exploited. However, Microsoft has acknowledged that a proof-of-concept for the flaw has been made public. Aspire recommendations patching this vulnerability immediately.

Aspire Protects

- **Apply Patches**: Ensure all systems are patched with the latest security updates. See Microsoft's security advisory for patch guidance.
- Monitor for suspicious activity related to PowerShell commands or unauthorized deployment of web shells.
- Regularly review password policies and enforce multi-factor authentication (MFA) to help prevent credential theft.

IoCs

- Suspicious traffic involving Microsoft Exchange servers
- Presence of the 'StealHook' backdoor or 'ngrok' tool on systems
- Unexplained password change events or interceptions

TTPs to Watch

- **Privilege Escalation**
  - Exploitation for Privilege Escalation (T1068**)** – Attackers exploit the Windows privilege escalation vulnerability (CVE-2024-30088) to elevate their privileges to the SYSTEM level on compromised devices.
- **Credential Access**
  - Input Capture (T1056) – OilRig registers a password filter DLL to intercept plaintext credentials during password change events.
  - Credential Dumping (T1003) – Attackers use the StealHook backdoor to capture credentials from Microsoft Exchange servers and exfiltrate them via email.

Aspire's 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 cyberattacks.
- **Aspire Managed Security Services**
  - Aspire Managed Security Services provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates "noise" and make sense of what really matters.
  - Our managed security portfolio includes:
    - Managed Firewall
    - Managed IDS/IPS
    - Security event monitoring & incident management
    - Managed Cisco ISE (Identity Services Engine)
    - Endpoint Protection

Supporting Documentation

CVE-2024-30088 - Security Update Guide - Microsoft - Windows Kernel Elevation of Privilege Vulnerability

CVE Website

Earth Simnavaz Levies Advanced Cyberattacks Against UAE and Gulf Regions | Trend Micro (US)