LevelBlue

# Incident Response & Digital Forensics

Monthly Threat Review - April 2025

# Agenda

## New Vulnerabilities

- Microsoft Security Update Overview
- Recent security updates from:
  - Adobe
  - Apple
  - Google
  - Cisco
  - SAP
  - Vmware
  - Palo Alto
- Known Exploited Vulnerabilities Catalog

## Prevalent Threats

- Update on the top 5 ransomware groups

# New Vulnerabilities

# Microsoft Security Update: April 2025

Total CVE's: 121 Critical: 11 Actively Exploited 1

## Actively Exploited

| CVE | Title | Severity |
|---|---|---|
| CVE-2025-29824 | Windows Common Log File System Driver Elevation of Privilege Vulnerability | Important |

## Critical Rated CVEs

| CVE | Title | Severity |
|---|---|---|
| CVE-2025-26663 | Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability | Critical |
| CVE-2025-26670 | Windows Lightweight Directory Access Protocol (LDAP) Client Remote Code Execution Vulnerability | Critical |
| CVE-2025-27480 | Windows Remote Desktop Services Remote Code Execution Vulnerability | Critical |
| CVE-2025-27482 | Windows Remote Desktop Services Remote Code Execution Vulnerability | Critical |
| CVE-2025-26686 | Windows TCP/IP Remote Code Execution Vulnerability | Critical |
| CVE-2025-27491 | Windows Hyper-V Remote Code Execution Vulnerability | Critical |
| CVE-2025-27745 | Microsoft Office Remote Code Execution Vulnerability | Critical |
| CVE-2025-27748 | Microsoft Office Remote Code Execution Vulnerability | Critical |
| CVE-2025-27749 | Microsoft Office Remote Code Execution Vulnerability | Critical |
| CVE-2025-27752 | Microsoft Office Remote Code Execution Vulnerability (Excel) | Critical |
| CVE-2025-29791 | Microsoft Office Remote Code Execution Vulnerability (Excel) | Critical |

# Microsoft Security Update: April 2025

Total CVE’s: 121 Critical: 11 Actively Exploited 1

## High Interest CVEs

| CVE | Title | Severity | Likelihood of Exploit |
|---|---|---|---|
| CVE-2025-26663 | Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability | Critical | Exploitation More Likely |
| CVE-2025-26670 | Windows Lightweight Directory Access Protocol (LDAP) Client Remote Code Execution Vulnerability | Critical | Exploitation More Likely |
| CVE-2025-27480 | Windows Remote Desktop Services Remote Code Execution Vulnerability | Critical | Exploitation More Likely |
| CVE-2025-27482 | Windows Remote Desktop Services Remote Code Execution Vulnerability | Critical | Exploitation More Likely |
| CVE-2025-27745 | Microsoft Office Remote Code Execution Vulnerability | Critical | Exploitation More Likely |
| CVE-2025-27748 | Microsoft Office Remote Code Execution Vulnerability | Critical | Exploitation More Likely |
| CVE-2025-27749 | Microsoft Office Remote Code Execution Vulnerability | Critical | Exploitation More Likely |
| CVE-2025-27752 | Microsoft Office Remote Code Execution Vulnerability (Excel) | Critical | Exploitation More Likely |
| CVE-2025-29791 | Microsoft Office Remote Code Execution Vulnerability (Excel) | Critical | Exploitation More Likely |
| CVE-2025-27472 | Windows Mark of the Web (MotW) Security Feature Bypass Vulnerability | Important | Exploitation More Likely |

# Additional Vendor Security Disclosures - April 2025

## Adobe

- Thirty-two (32) vulnerabilities addressed, including fifteen (15) critical.
- Acrobat, Reader, Photoshop impacted.
- No active exploits reported.

## Apple

- Two (2) actively exploited vulnerabilities in WebKit and kernel.
- Active exploits:
- CVE-2025-24201: WebKit out-of-bounds write in JavaScriptCore, affecting memory management during JavaScript execution (iOS 18.4, macOS Sequoia 15.4).
- CVE-2025-24202: Kernel privilege escalation via Mach message handling in XNU, enabling root access (macOS Sequoia 15.4).
- iOS 18.4.1, iPadOS 18.4.1, macOS Sequoia 15.4.1 released.

## Google

- Thirty-eight (38) vulnerabilities patched in Android and Chrome.
- One (1) actively exploited vulnerability.
- Active exploit:
- CVE-2025-24309: Chrome use-after-free in Blink rendering engine's DOM handling, tied to V8 JavaScript execution.
- Android 15 April update, Chrome 124.0.6367.91 released.

## Cisco

- Twelve (12) vulnerabilities in network management products.
- One (1) actively exploited vulnerability.
- **Active exploit:**
- CVE-2025-20182: Cisco Secure Firewall command injection in CLI parser, allowing root command execution.
- Secure Firewall, Nexus Dashboard patched.

## SAP

- Eight (8) vulnerabilities addressed, including three (3) critical.
- BusinessObjects, NetWeaver impacted.
- No active exploits reported.

## VMWare

- Five (5) vulnerabilities, one (1) actively exploited.
- **Active exploit:**
- CVE-2025-22229: ESXi sandbox escape via VMX process, exploiting hypercall interface for host access.
- ESXi, vCenter, Workstation patched.

## Palo Alto

- Three (3) vulnerabilities in PAN-OS.
- One (1) actively exploited vulnerability.
- Active exploit:
- CVE-2025-0109: PAN-OS authentication bypass in management web interface's PHP session handling, targeting GlobalProtect.
- GlobalProtect, Expedition targeted.

# U.S. Cybersecurity Infrastructure Security Agency

## Known Exploited Vulnerabilities Catalog

| CVE | Vendor | Product | Description | Date |
|---|---|---|---|---|
| CVE-2025-29824 | Microsoft | Windows CLFS Driver | Elevation of privilege via use-after-free in CLFS, enabling SYSTEM-level access for ransomware deployment. | 4/8/25 |
| CVE-2025-24201 | Apple | WebKit | Out-of-bounds write in JavaScriptCore allows arbitrary code execution via malicious web content. | 4/10/25 |
| CVE-2025-24202 | Apple | macOS Kernel | Privilege escalation via Mach message handling in XNU, granting root access on macOS Sequoia. | 4/10/25 |
| CVE-2025-24309 | Google | Chrome | Use-after-free in Blink rendering engine enables code execution through malicious webpages. | 4/12/25 |
| CVE-2025-20182 | Cisco | Secure Firewall | Command injection in CLI parser allows root command execution on the firewall. | 4/15/25 |
| CVE-2025-22229 | VMware | ESXi | Sandbox escape via VMX process allows host-level code execution on ESXi servers. | 4/18/25 |
| CVE-2025-0109 | Palo Alto | PAN-OS | Authentication bypass in management web interface enables unauthorized administrative access. | 4/20/25 |

# General Recommendations

- Apply patches provided by product vendors to vulnerable systems immediately after thorough testing.
- Run all software with non-administrative privileges to reduce the impact of a successful attack.
- Advise users to avoid visiting untrusted websites or clicking links from unknown or untrusted sources. Consider setting up email filtering to block HTTP links, minimizing the risk of users accidentally accessing malicious content.
- If blocking URL links isn't feasible, educate users about the dangers of hypertext links in emails or attachments, particularly from untrusted sources.
- Implement the principle of Least Privilege across all systems and services.

# Prevalent Threats

# Prevalent Threats

Top threat groups

- Akira
- satanlock
- qilin
- play
- nighspire

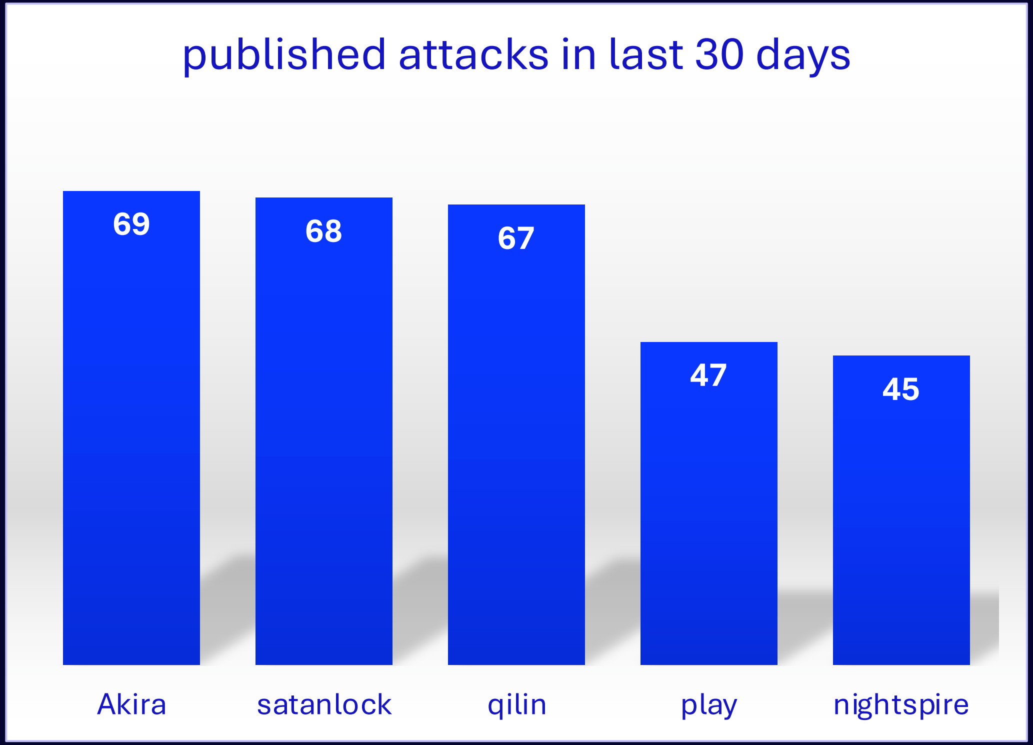
Threat Group Highlight

satanlock

- Appeared this month (April 2025)
- Analysis suggests is connected to GD Lockersec and Babuk-Bjorka

Nightspire

- First appeared in March 2025
- Targted CVE 2024-55591 Fortinet firewalls to gain access



data from information published on threat group leak sites

# Thank you