LevelBlue

Incident Response & Digital Forensics

Monthly Threat Review - March 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: March 2025

Total CVE's: 57 Critical: 6 Actively Exploited 6

Actively Exploited

CVE	Title	Severity
CVE-2025-24983	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Important
CVE-2025-24984	Windows NTFS Information Disclosure Vulnerability	Important
CVE-2025-24985	Windows Fast FAT File System Driver Integer Overflow Vulnerability	Important
CVE-2025-24991	Windows NTFS Out-Of-Bounds Read Vulnerability	Important
CVE-2025-24993	Windows NTFS Heap-Based Buffer Overflow Vulnerability	Important
CVE-2025-26633	Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability	Important

Zero-Day (Publicly Disclosed, Not Actively Exploited)

CVE	Title	Severity
CVE-2025-22237	Microsoft Edge (Chromium-based) Security Feature Bypass	Important

Critical Rated CVEs

CVE	Title	Severity
CVE-2025-26645	Windows Remote Desktop Services Remote Code Execution Vulnerability	Critical
CVE-2025-24045	Windows Remote Desktop Services Remote Code Execution Vulnerability	Critical
CVE-2025-24035	Windows Remote Desktop Services Remote Code Execution Vulnerability	Critical
CVE-2025-24084	Windows Subsystem for Linux (WSL2) Remote Code Execution Vulnerability	Critical
CVE-2025-24064	Windows Domain Name Service (DNS) Remote Code Execution Vulnerability	Critical
CVE-2025-24057	Microsoft Office Remote Code Execution Vulnerability	Critical

Microsoft Security Update: March 2025

Total CVE's: 57 **Critical: 6** **Actively Exploited 6**

High Interest CVEs

CVE	Title	Severity	Likelihood of Exploit
CVE-2025-24035	Windows Remote Desktop Services Remote Code Execution Vulnerability	Critical	Exploitation More Likely
CVE-2025-24983	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Important	Exploitation More Likely
CVE-2025-24984	Windows NTFS Information Disclosure Vulnerability	Important	Exploitation More Likely
CVE-2025-24985	Windows Fast FAT File System Driver Integer Overflow Vulnerability	Important	Exploitation More Likely
CVE-2025-24991	Windows NTFS Out-Of-Bounds Read Vulnerability	Important	Exploitation More Likely
CVE-2025-24993	Windows NTFS Heap-Based Buffer Overflow Vulnerability	Important	Exploitation More Likely
CVE-2025-26633	Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability	Important	Exploitation More Likely
CVE-2025-22237	Microsoft Edge (Chromium-based) Security Feature Bypass	Important	Exploitation More Likely
CVE-2025-26645	Remote Desktop Client Remote Code Execution Vulnerability	Critical	Exploitation More Likely
CVE-2025-24045	Windows Remote Desktop Services Remote Code Execution Vulnerability	Critical	Exploitation More Likely
CVE-2025-24084	Windows Subsystem for Linux (WSL2) Remote Code Execution Vulnerability	Critical	Exploitation More Likely

Additional Vendor Security Disclosures - Mar 2025

Adobe

- Forty (40) vulnerabilities addressed including twenty (20) critical.
- Acrobat, Reader, Experience Manager impacted.
- No active exploits.

Apple

- One (11) Actively exploited bug in WebKit (out-of-bands write)
- Active exploits
  CVE 2025-24201 Webkit
- iOS and iPadOS 18.4 | macOS Sequoia 15.4

Google

- Forty-four (44) vulnerabilities patched in Android.
- Two (2) actively exploited vulnerabilities
- CVE-2024-43093: Privilege escalation in Framework.
  CVE-2024-50302: Privilege escalation in Linux kernel HID USB.

Cisco

- One (1) active exploited
- CVE-2023-20118 Small Business RV Series Routers Command Injection.

SAP

- None

VMWare

- Three (3) vulnerabilities actively exploited.
- CVE-2025-22225 ESXi Arbitrary Write.
- CVE-2025-22224 ESXi/Workstation TOCTOU Race Condition.
- CVE-2025-22226 ESXi/Workstation/Fusion Information Disclosure.

Palo Alto

- Two (2) vulnerabilities in PAN-OS.
- Active exploits:
  CVE-2025-0108 Authentication Bypass.
  CVE-2025-0111 File Read.
- Management web interface targeted.

U.S. Cybersecurity Infrastructure Security Agency

Known Exploited Vulnerabilities Catalog

CVE	Vendor	Product	Description	Date
CVE-2025-24989	Microsoft	Power Pages	Improper access control allows unauthorized access to sensitive data or functionality.	2/21/25
CVE-2017-3066	Adobe	ColdFusion	Deserialization vulnerability enables arbitrary code execution via untrusted data.	2/24/25
CVE-2024-49035	Microsoft	Partner Center	Improper access control permits unauthorized access to Partner Center resources.	2/24/25
CVE-2023-34192	Synacor	Zimbra Collaboration Suite	Cross-Site Scripting (XSS) allows script execution in user's browser context.	2/24/25
CVE-2023-20118	Cisco	Small Business RV Series Routers	Command injection via improper input sanitization enables arbitrary OS command execution.	3/2/25
CVE-2022-43939	Hitachi Vantara	Pentaho BA Server	Authorization bypass allows unauthorized access to server resources.	3/2/25
CVE-2022-43769	Hitachi Vantara	Pentaho BA Server	Special element injection enables unauthorized data manipulation on the server.	3/2/25
CVE-2018-8639	Microsoft	Windows Win32k	Improper resource shutdown allows privilege escalation via Win32k component.	3/2/25
CVE-2024-4885	Progress	WhatsUp Gold	Path traversal vulnerability allows unauthorized access to arbitrary files.	3/2/25
CVE-2024-50302	Linux (Google Android)	Kernel HID USB	Privilege escalation via uninitialized kernel memory leak in HID USB component.	3/3/25
CVE-2025-22224	VMware	ESXi/Workstation	TOCTOU race condition leads to out-of-bounds write, enabling code execution on the host.	3/3/25
CVE-2025-22225	VMware	ESXi	Arbitrary write allows code execution as VMX process on the host.	3/3/25
CVE-2025-22226	VMware	ESXi/Workstation/Fusion	Information disclosure enables extraction of sensitive hypervisor data.	3/3/25
CVE-2025-25181	Advantive	VeraCore	SQL injection allows unauthorized database access and manipulation.	3/9/25
CVE-2024-57968	Advantive	VeraCore	Unrestricted file upload enables arbitrary file execution on the server.	3/9/25

U.S. Cybersecurity Infrastructure Security Agency

Known Exploited Vulnerabilities Catalog

CVE	Vendor	Product	Description	Date
CVE-2024-13159	Ivanti	Endpoint Manager	Path traversal allows unauthorized access to arbitrary files on the server.	3/9/25
CVE-2024-13160	Ivanti	Endpoint Manager	Path traversal enables unauthorized file access on the server.	3/9/25
CVE-2024-13161	Ivanti	Endpoint Manager	Path traversal permits unauthorized access to sensitive files.	3/9/25
CVE-2025-24983	Microsoft	Windows Win32k	Use-after-free vulnerability enables privilege escalation in Win32k component.	3/10/25
CVE-2025-24984	Microsoft	Windows NTFS	Information disclosure allows unauthorized access to heap memory via NTFS.	3/10/25
CVE-2025-24985	Microsoft	Windows Fast FAT File System	Integer overflow in Fast FAT driver enables local code execution.	3/10/25
CVE-2025-24991	Microsoft	Windows NTFS	Out-of-bounds read in NTFS allows unauthorized data access.	3/10/25
CVE-2025-24993	Microsoft	Windows NTFS	Heap-based buffer overflow in NTFS enables privilege escalation.	3/10/25
CVE-2025-26633	Microsoft	Windows Management Console	Improper neutralization allows remote code execution via untrusted data.	3/10/25

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

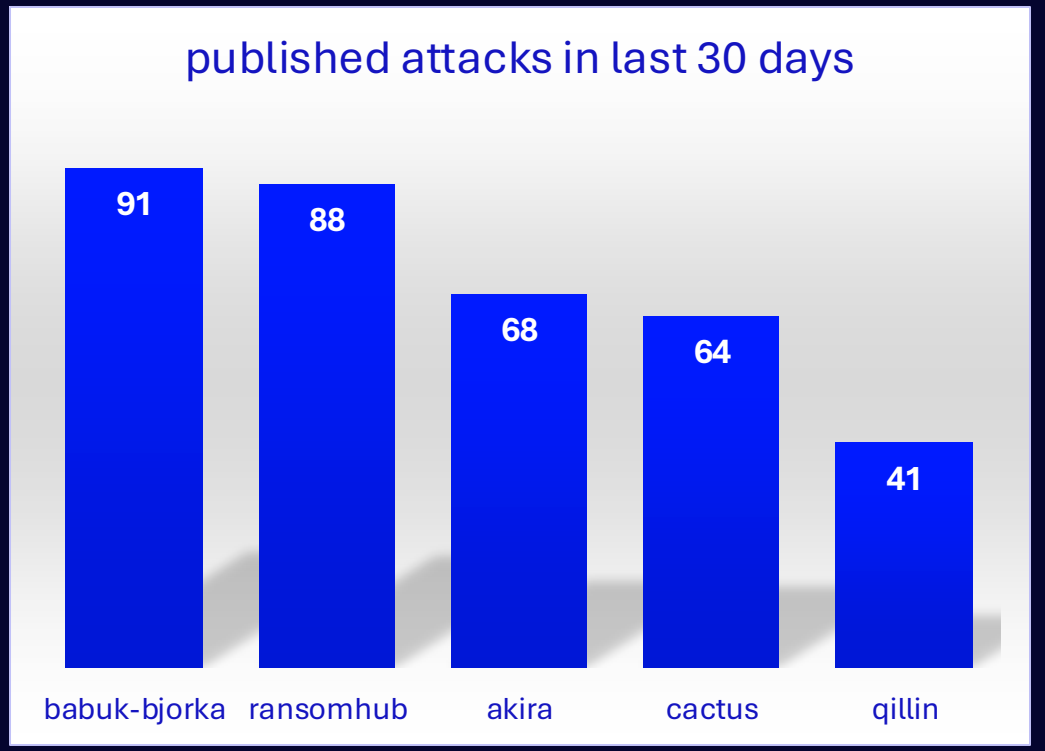
Top threat groups

- babuk-bjorka
- ransomhub
- akira
- play
- lynx

Threat Group Highlight

Babuk-Bjorka (Babuk2)

- Emerged in late 2024, relaunched DLS on January 26, 2025.
- Operates as Babuk2, led by admin Bjorka.
- No confirmed link to original Babuk (active 2021–2022).



data from information published on threat group leak sites

https://www.proofpoint.com/us/blog/threat-insight/security-brief-millions-messages-distribute-lockbit-black-ransomware
https://www.bleepingcomputer.com/news/security/ransomware-gang-targets-windows-admins-via-putty-winscp-malvertising/

Thank you

Our next update is Apr 24th, 2025