LevelBlue

Incident Readiness & Response Monthly Briefing

Monthly Threat Review - February 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
- clop ransomware surge

New Vulnerabilities

Microsoft Security Update: February 2025

Total CVE’s: 67 Critical: 4 Actively Exploited 2

Actively Exploited

CVE	Title	Severity
CVE-2025-21418	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability (AFD.sys)	Important
CVE-2025-21391	Windows Storage Elevation of Privilege Vulnerability	Important

Zero-Day (Publicly Disclosed, Not Actively Exploited)

CVE-2025-21377	Microsoft Account Privilege Escalation NTLM Hash Disclosure Spoofing	Important
CVE-2025-21194	Microsoft Surface Security Feature Bypass	Important

Critical Rated CVEs

CVE	Title	Severity
CVE-2025-21376	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	Critical
CVE-2025-21381	Microsoft Excel Remote Code Execution Vulnerability	Critical
CVE-2025-21379	DHCP Client Service Remote Code Execution Vulnerability	Critical
CVE-2025-21415	Azure AI Face Service Authentication Bypass by Spoofing **out of band patch on Feb 4, 2025	Critical

Microsoft Security Update: February 2025

Total CVE's: 67 **Critical: 4** **Actively Exploited 2**

High Interest CVEs

CVE	Title	Severity	Likelihood of exploit
CVE-2025-21414	Windows Core Messaging Elevation of Privileges Vulnerability	Important	Exploitation More Likely
CVE-2025-21184	Azure Network Watcher VM Extension Elevation of Privilege Vulnerability	Important	Exploitation More Likely
CVE-2025-21400	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important	Exploitation More Likely
CVE-2025-21377	NTLM Hash Disclosure Spoofing Vulnerability	Important	Exploitation More Likely
CVE-2025-21367	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Important	Exploitation More Likely
CVE-2025-21420	Windows Disk Cleanup Tool Elevation of Privilege Vulnerability	Important	Exploitation More Likely
CVE-2025-21419	Windows Setup Files Cleanup Elevation of Privilege Vulnerability	Important	Exploitation More Likely
CVE-2025-21376	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	Critical	Exploitation More Likely

Additional Vendor Security Disclosures - Feb 2025

Adobe

- Forty-Five (45) vulnerabilities addressed including twenty-three (23) critical.
- Adobe InDesign, Commerce, Substance 3D Stager, InCopy, Illustrator, Substance 3D Designer, and Photoshop Elements.
- No active exploits.

Apple

- Fourteen (14) vulnerabilities patched across all product lines.
- Active exploits
  - CoreMedia Use-After-Free Privilege Escalation (CVE 2025-24085)
  - USB Restricted Mode Bypass (CVE 2025-24200)
- iOS and iPadOS 18.3.1 | iOS and iPadOS 17.7.5 | macOS Sequoia 15.3.1

Google

- Fourth-seven (47) vulnerabilities addressed. Critical vulnerability in Qualcomm WLAN.
- Active exploit of Kernel USB Driver (CVE 2025-53104).
- Chrome version 133

Cisco

- Seventeen (17) security vulnerabilities patched
- Two (2) critical vulnerabilities in the Cisco Identity Service Engine
- No active exploits

SAP

- Nineteen (19) security notes. Six (6) identified as critical
- Critical vulnerabilities in NetWeaver | Business Objects | Supplier Relationship Management | AppRouter

VMWare

- None reported

Palo Alto

- Five (5) vulnerabilities identified in "Expedition Migration Tool"
- Two (2) Critical vulnerabilities
  - OS Command Injection | SQL Injection | Cross-Site Scripting
  - Threat actor could gain access to network device credentials
- Latest version 1.2.96 addresses vulnerabilities
- Product reached end-of-life (EoL) on Dec 31, 2024

U.S. Cybersecurity Infrastructure Security Agency

Known Exploited Vulnerabilities Catalog

CVE	Vendor	Product	Description	Date
CVE-2025-0411	7-Zip	7-Zip	7-Zip contains a protection mechanism failure vulnerability that allows remote attackers to bypass the Mark-of-the-Web security feature to execute arbitrary code in the context of the current user.	2/6/25
CVE-2024-45195	Apache	OFBiz	Apache OFBiz contains a forced browsing vulnerability that allows a remote attacker to obtain unauthorized access.	2/4/25
CVE-2024-29059	Microsoft	.NET Framework	Microsoft .NET Framework contains an information disclosure vulnerability that exposes the ObjRef URI to an attacker, ultimately enabling remote code execution.	2/4/25
CVE-2018-19410	Paessler	PRTG Network Monitor	Paessler PRTG Network Monitor contains a local file inclusion vulnerability that allows a remote, unauthenticated attacker to create users with read-write privileges (including administrator).	2/4/25
CVE-2018-9276	Paessler	PRTG Network Monitor	Paessler PRTG Network Monitor contains an OS command injection vulnerability that allows an attacker with administrative privileges to execute commands via the PRTG System Administrator web console.	2/4/25
CVE-2024-53104	Linux	Kernel	Linux kernel contains an out-of-bounds write vulnerability in the uvc_parse_streaming component of the USB Video Class (UVC) driver that could allow for physical escalation of privilege.	2/5/25
CVE-2020-29574	Sophos	CyberoamOS	CyberoamOS (CROS) contains a SQL injection vulnerability in the WebAdmin that allows an unauthenticated attacker to execute arbitrary SQL statements remotely.	2/6/25
CVE-2022-23748	Audinate	Dante Discovery	Dante Discovery contains a process control vulnerability in mDNSResponder.exe that all allows for a DLL sideloading attack. A local attacker can leverage this vulnerability in the Dante Application Library to execute arbitrary code.	2/6/25
CVE-2024-21413	Microsoft	Office Outlook	Microsoft Outlook contains an improper input validation vulnerability that allows for remote code execution. Successful exploitation of this vulnerability would allow an attacker to bypass the Office Protected View and open in editing mode rather than protected mode.	2/6/25
CVE-2020-15069	Sophos	XG Firewall	Sophos XG Firewall contains a buffer overflow vulnerability that allows for remote code execution via the "HTTP/S bookmark" feature.	2/6/25
CVE-2025-0994	Trimble	Cityworks	Trimble Cityworks contains a deserialization vulnerability. This could allow an authenticated user to perform a remote code execution attack against a customer's Microsoft Internet Information Services (IIS) web server.	2/7/25
CVE-2025-21418	Microsoft	Windows	Microsoft Windows Ancillary Function Driver for WinSock contains a heap-based buffer overflow vulnerability that allows for privilege escalation, enabling a local attacker to gain SYSTEM privileges.	2/11/25
CVE-2025-21391	Microsoft	Windows	Microsoft Windows Storage contains a link following vulnerability that could allow for privilege escalation. This vulnerability could allow an attacker to delete data including data that results in the service being unavailable.	2/11/25
CVE-2024-40890	Zyxel	DSL CPE Devices	Multiple Zyxel DSL CPE devices contain a post-authentication command injection vulnerability in the CGI program that could allow an authenticated attacker to execute OS commands via a crafted HTTP request.	2/11/25
CVE-2024-40891	Zyxel	DSL CPE Devices	Multiple Zyxel DSL CPE devices contain a post-authentication command injection vulnerability in the management commands that could allow an authenticated attacker to execute OS commands via Telnet.	2/11/25

U.S. Cybersecurity Infrastructure Security Agency

Known Exploited Vulnerabilities Catalog

CVE	Vendor	Product	Description	Date
CVE-2025-24200	Apple	iOS and iPadOS	Apple iOS and iPadOS contains an incorrect authorization vulnerability that allows a physical attacker to disable USB Restricted Mode on a locked device.	2/12/25
CVE-2024-41710	Mitel	SIP Phones	Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, contain an argument injection vulnerability due to insufficient parameter sanitization during the boot process. Successful exploitation may allow an attacker to execute arbitrary commands within the context of the system.	2/12/25
CVE-2024-57727	SimpleHelp	SimpleHelp	SimpleHelp remote support software contains multiple path traversal vulnerabilities that allow unauthenticated remote attackers to download arbitrary files from the SimpleHelp host via crafted HTTP requests. These files may include server configuration files and hashed user passwords.	2/13/25
CVE-2025-0108	Palo Alto Networks	PAN-OS	Palo Alto Networks PAN-OS contains an authentication bypass vulnerability in its management web interface. This vulnerability allows an unauthenticated attacker with network access to the management web interface to bypass the authentication normally required and invoke certain PHP scripts.	2/18/25
CVE-2024-53704	SonicWall	SonicOS	SonicWall SonicOS contains an improper authentication vulnerability in the SSLVPN authentication mechanism that allows a remote attacker to bypass authentication.	2/18/25
CVE-2025-23209	Craft CMS	Craft CMS	Craft CMS contains a code injection vulnerability caused by improper validation of the database backup path, ultimately enabling remote code execution.	2/20/25
CVE-2025-0111	Palo Alto Networks	PAN-OS	Palo Alto Networks PAN-OS contains an external control of file name or path vulnerability. Successful exploitation enables an authenticated attacker with network access to the management web interface to read files on the PAN-OS filesystem that are readable by the ,Äúnobody,Äù user.	2/20/25
CVE-2025-24989	Microsoft	Power Pages	Microsoft Power Pages contains an improper access control vulnerability that allows an unauthorized attacker to elevate privileges over a network potentially bypassing the user registration control.	2/21/25
CVE-2017-3066	Adobe	ColdFusion	Adobe ColdFusion contains a deserialization vulnerability in the Apache BlazeDS library that allows for arbitrary code execution.	2/24/25
CVE-2024-20953	Oracle	Agile Product Lifecycle Management (PLM)	Oracle Agile Product Lifecycle Management (PLM) contains a deserialization vulnerability that allows a low-privileged attacker with network access via HTTP to compromise the system.	2/24/25
CVE-2024-49035	Microsoft	Partner Center	Microsoft Partner Center contains an improper access control vulnerability that allows an attacker to escalate privileges.	2/25/25
CVE-2023-34192	Synacor	Zimbra Collaboration Suite (ZCS)	Synacor Zimbra Collaboration Suite (ZCS) contains a cross-site scripting (XSS) vulnerability that allows a remote authenticated attacker to execute arbitrary code via a crafted script to the /h/autoSaveDraft function.	2/25/25

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

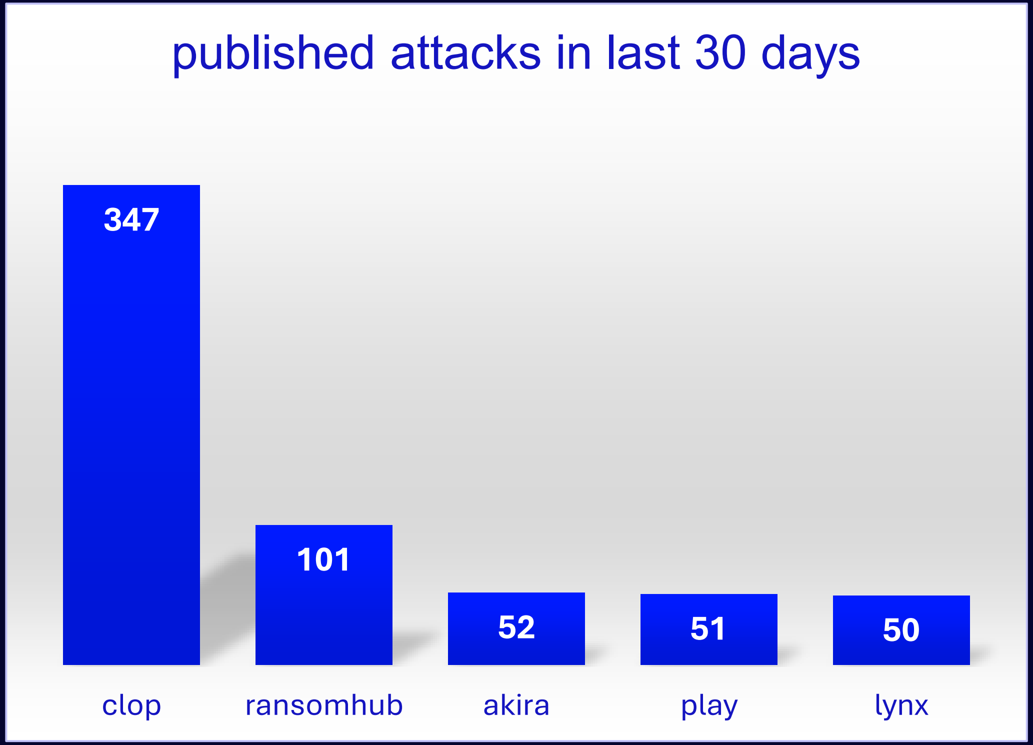
Top threat groups

- clop
- ransomhub
- akira
- play
- lynx

Threat Group Highlight

Clop threat group operations continues to surge

File transfer software needs to be at the top of any patch management operational plan



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 Mar 28th, 2025