Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Zero-Day in WinRAR Actively Weaponized by Multiple Threat Groups

Date of Publication	Admiralty Code	TA Number
August 12, 2025	A1	TA2025247

Summary

First Seen: July 18, 2025
Affected Product: RARLAB WinRAR
Affected Platform: Windows
Targeted Industries: Financial, Manufacturing, Defense, Logistics
Targeted Region: Europe, Canada, Russia
Actor: RomCom (aka Tropical Scorpius, Void Rabisu, DEV-0978, Storm-0978, UNC2596, CIGAR, UAC-0180), Paper Werewolf (aka GOFFEE)
Impact: A newly discovered zero-day flaw in WinRAR, tracked as CVE-2025-8088, has been actively exploited in targeted attacks, with threat groups like RomCom and Paper Werewolf using it to deliver malicious payloads through seemingly harmless RAR archives. The vulnerability, found in the Windows version of WinRAR, allows attackers to exploit path traversal via alternate data streams, enabling them to plant harmful files in sensitive locations. RomCom used spear-phishing campaigns against European and Canadian companies, deploying multi-stage attack chains that delivered malware including Mythic agents, SnipBot variants, and RustyClaw downloaders. Paper Werewolf threat actor purchased the exploit for $80,000 and targeted Russian organizations, sometimes chaining it with another WinRAR flaw. WinRAR has since patched the issue in version 7.13, making prompt updates essential to prevent compromise.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-8088	RARLAB WinRAR Path Traversal Vulnerability	RARLAB WinRAR	✓	✗	✓
CVE-2025-6218	RARLAB WinRAR Directory Traversal Remote Code Execution Vulnerability	RARLAB WinRAR	✗	✗	✓

Vulnerability Details

#1

A critical zero-day vulnerability in WinRAR, tracked as CVE-2025-8088, has come under active exploitation in a wave of targeted cyberattacks. The flaw, which affects Windows versions of WinRAR and its associated components like UnRAR.dll, arises from improper handling of alternate data streams (ADSes) in specially crafted archive files. By manipulating file paths within these ADSes, attackers can perform path traversal, tricking WinRAR into extracting malicious files outside the intended directory.

#2

The vulnerability first drew attention on July 18, 2025, when researchers discovered a malicious DLL named msedge.dll inside a RAR archive exploiting the flaw. The campaign was linked to RomCom, a Russia-aligned threat actor known for leveraging zero-days. In this case, the attackers-built archives containing one harmless-looking file alongside numerous malicious ADS entries. These were unpacked and set to execute on login, with the attackers cleverly padding the archive with dummy data and invalid paths to evade detection only revealing the malicious entries when scrolling deep into the WinRAR interface.

#3

From July 18, RomCom was deploying RAR files against companies in Europe and Canada. The archives contained two malicious files, an LNK shortcut and a DLL leading to three identified execution chains. In the first, Updater.lnk planted a registry key pointing to msedge.dll, triggering its execution through COM hijacking. The DLL decrypted AES-protected shellcode, checked for a specific domain match, and, if confirmed, connected to a Mythic C2 server. The second chain used Display Settings.lnk to run ApbxHelper.exe, a tampered PuTTY CAC binary which decrypted and executed SnipBot shellcode if certain registry conditions were met, eventually downloading another payload. The third chain featured RustyClaw, a Rust-based downloader signed with an invalid certificate, fetching a payload from melamorri[.]com.

#4

Paper Werewolf, another threat group, also used the exploit, possibly after purchasing it from a dark web vendor offering it for $80,000. Unlike RomCom's campaigns, Paper Werewolf targeted Russian organizations, chaining CVE-2025-8088 with an earlier WinRAR flaw, CVE-2025-6218, in phishing operations. This cross-actor exploitation highlights how valuable and quickly circulated a working zero-day can be within the cybercrime ecosystem.

#5

Given the active exploitation and the breadth of sectors targeted, users are urged to upgrade immediately to WinRAR 7.13 or later, which includes fixes for CVE-2025-8088 and other security issues.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-8088	WinRAR Versions up to and including 7.12	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*:*	CWE-35
CVE-2025-6218	WinRAR Version Prior to 7.12	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*:*	CWE-22

Recommendations

- **Update WinRAR immediately:** Install WinRAR version 7.13 or later, which fixes CVE-2025-8088 and other security flaws. This is the single most effective step to block these attacks.
- **Be cautious with unexpected archives:** Avoid opening RAR or ZIP files from unknown or untrusted sources, even if they seem harmless or come from someone you know (email accounts can be compromised).
- **Check for suspicious startup items:** Since this exploit can drop malicious files into the Windows Startup folder, review your startup programs regularly and remove anything unfamiliar.
- **Use strong endpoint protection:** Ensure your antivirus or endpoint detection software is up to date and consider enabling real-time scanning to detect suspicious DLL or LNK activity.
- **Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact
T1583 Acquire Infrastructure	T1587 Develop Capabilities	T1587.001 Malware	T1587.004 Exploits
T1588 Obtain Capabilities	T1588.005 Exploits	T1588.006 Vulnerabilities	T1608 Stage Capabilities
T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution	T1204.002 Malicious File
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1546 Event Triggered Execution	T1546.015 Component Object Model Hijacking
T1497 Virtualization/Sandbox Evasion	T1480 Execution Guardrails	T1036 Masquerading	T1036.001 Invalid Code Signature
T1027 Obfuscated Files or Information	T1027.007 Dynamic API Resolution	T1027.013 Encrypted/Encoded File	T1555 Credentials from Password Stores
T1555.003 Credentials from Web Browsers	T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1087 Account Discovery

T1518 Software Discovery	T1021 Remote Services	T1560 Archive Collected Data	T1185 Browser Session Hijacking
T1005 Data from Local System	T1114 Email Collection	T1114.001 Local Email Collection	T1113 Screen Capture
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography
T1041 Exfiltration Over C2 Channel	T1657 Financial Theft	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell
T1658 Exploitation for Client Execution	T1564 Hide Artifacts	T1564.003 Hidden Window	T1027.009 Embedded Payloads
T1082 System Information Discovery	T1033 System Owner/User Discovery	T1105 Ingress Tool Transfer	T1095 Non-Application Layer Protocol
T1574 Hijack Execution Flow	T1574.001 DLL		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	371A5B8BA86FBCAB80D4E0087D2AA0D8FFDDC70B, D43F49E6A586658B5422EDC647075FFD405D6741, F77DBA76010A9988C9CEB8E420C96AEBC071B889, 676086860055F6591FED303B4799C725F8466CF4, 1F25E062E8E9A4F1792C3EAC6462694410F0F1CA, C340625C779911165E3983C77FD60855A2575275, C94A6BD6EC88385E4E831B208FED2FA6FAED6666, 01D32FE88ECDEA2B934A00805E138034BF85BF83, AE687BEF963CB30A3788E34CC18046F54C41FFBA, AB79081D0E26EA278D3D45DA247335A545D0512E, 1AEA26A2E2A7711F89D06165E676E11769E2FD68, 40e647d61a00fd7240e54dba45ce95c5d33cae43, 7ff3d32e78c5626135a73bba4a011058f714ae86, d3820a1248bf54ce8a3d05bf688bcd97e1c41d8e,

TYPE	VALUE
SHA1	6c0e52b8ed746b5b8ebef1ef2226093260659ae8, b610ff2ad9791d17203609d747c5dfe947304591, b7bba4a216f4910f5072019bb4a2022ccf098c75, 23708d1fdcd7ba65c2b2fc676cee707e746a2dd9
Filenames	Adverse_Effect_Medical_Records_2025.rar, cv_submission.rar, Eli_Rosenfeld_CV2-Copy(10).rar, Datos adjuntos sintítulo00170.dat, JobDocs_July2025.rar, cv_submission.rar, Recruitment_Dossier_July_2025.rar, install_module_x64.dll, msedge.dll, Complaint.exe, ApbxHelper.exe, minprom_04072025.rar, xpsrchvw.exe, Запрос_Минпромторг_22.07.rar, DON_AVIA_TRANS_UZ.rar, DON_AVIA_TRANS_RU.rar, WinRunApp.exe
IPv4	162[.]19[.]175[.]44, 194[.]36[.]209[.]127, 85[.]158[.]108[.]62, 185[.]173[.]235[.]134, 81[.]30[.]105[.]148, 213[.]171[.]4[.]200, 89[.]110[.]98[.]26, 94[.]242[.]51[.]73
IPv4:Port	89[.]110[.]88[.]155[:]8090
Domains	gohazeldale [.]com, srlaptop[.]com, melamorri[.]com, campanole[.]com, eliteheirs[.]org, indoorvisions[.]org, trailtastic[.]org
MD5	9a69b948e261363463da38bdbf828b14, 942220fc9382f44ae82061d1fc63f41e, 6b4d7a63aa2a8b2a5a3fbad6c8e6533e, eaba94b5237d2625fa38bc924e5347c4, d176b7b5040d7bb32bae4d5c3c3b6aaf, 1670035385c9031f79566c6f73fb9743, 67daddd8fd8a59c8b3d40ea433efd6ff

TYPE	VALUE
SHA256	fe2587dd8d9755b7b3a106b6e46519a1ce0a8191eb20821d2f957326dbf912e9, bf74820d40d281c28d5928b01e5b68d6caf85b5b9188bf4efb627765d708bcff, 28a2b98ae214376ccd549a8b0dccafad31c8b234d0b81a0e8817579566615567, d2c3fe8b9a4e0e5b7bcc087d52295ab30dc25b1410f50de35470383528c9d844, dfab2f25c9d870f30bbc4abb873d155cf4904ece536714fb9cd32b2e0126dfab, 2446f97c1884f70f97d68c2f22e8fc1b9b00e1559cd3ca540e8254749a693106, 236aba76d427111e8c140604ead9c4ab86264b1ae197fc26fadb33c46be94289
URLs	hxxps[:]//eliteheirs[.]org/checks/brandished/dyestuffs/abbess/interrelation?4eab27f5266393a1150e7d6453c1920db480c2f88ce96708cff593e38ae8ac30, hxxps[:]//eliteheirs[.]org/checks/brandished/dyestuffs/abbess/interrelation, hxxps[:]//eliteheirs[.]org/crossness/outpost/autocracies/decapitations/jetsetting?b115ef3ad9cb948213f7efc4876cf67747eac173b613b425abd05dba0e306ebd, hxxps[:]//eliteheirs[.]org/crossness/outpost/autocracies/decapitations/jetsetting, hxxps[:]//indoorvisions[.]org/patriarchal/furthering/creating/flared/censured?hostname=[hostname]&username=[username], hxxps[:]//indoorvisions[.]org/patriarchal/furthering/creating/flared/censured, hxxps[:]//trailtastic[.]org/glowworms/diverted/calorie/britons/parabolas?hostname=[hostname]&username=[username], hxxps[:]//trailtastic[.]org/glowworms/diverted/calorie/britons/parabolas
Mutexes	Sfgjh824nf6sdfgsfwe6467jkgg3vvvv3q7657fj436jh54HGFa56, Global_22576733

Patch Details

Install the latest version of WinRAR 7.13 or later to address the flaw.

Link: https://www.win-rar.com/download.html?&L=0

References

https://www.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=283&cHash=a64b4a8f662d3639dec8d65f47bc93c5

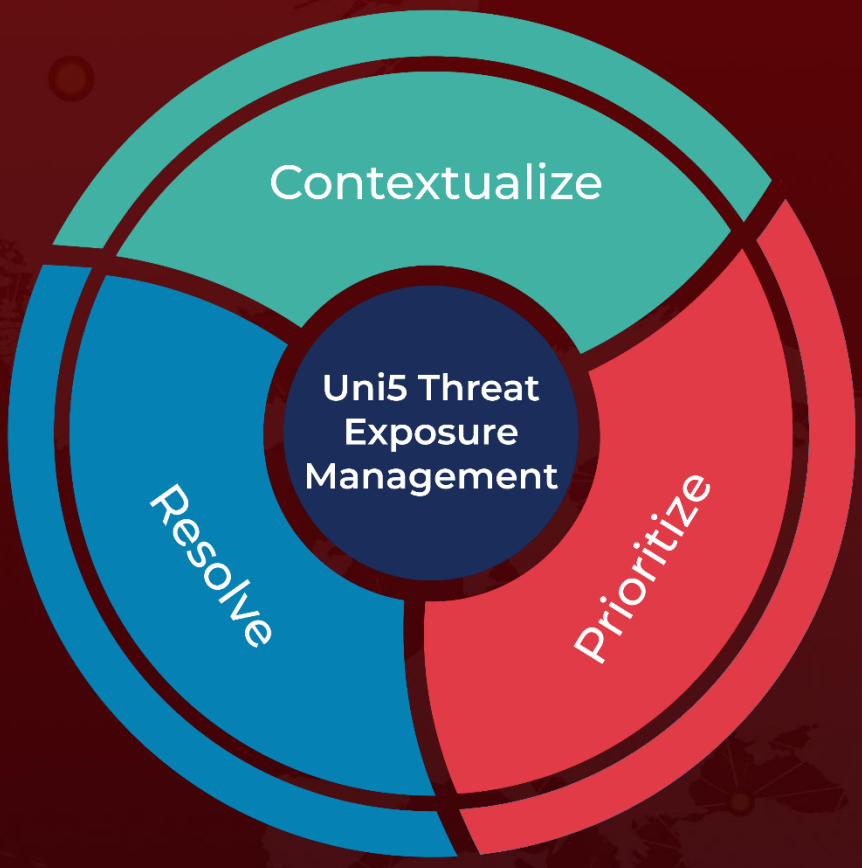
https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/

https://bi.zone/expertise/blog/paper-werewolf-atakuet-rossiyu-s-ispolzovaniem-uyazvimosti-nulevogo-dnya-v-winrar/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 12, 2025 • 7:20 AM

More at www.hivepro.com