Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

WinRAR Zero-Day Exploit Targeting Traders Since April

Date of Publication	Admiralty Code	TA Number
August 24, 2023	A1	TA2023343

Summary

First Seen: April, 2023
Malware: DarkMe, GuLoader, and Remcos RAT
Affected Platforms: RARLAB WinRAR
Impact: The zero-day vulnerability (CVE-2023-38831) in WinRAR, allowing hackers to install malware through manipulated archives, exposing users to hidden malicious scripts and potential cyberattacks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	RARLAB WinRAR	✓	✓	✓

Vulnerability Details

#1

A zero-day vulnerability in WinRAR, known as CVE-2023-38831, has been actively exploited by cybercriminals since April 2023. The vulnerability allowed hackers to distribute malware by creating seemingly harmless archives that contained files like JPG images, text documents, or PDFs. When users opened these files, the flaw triggered a script that installed malware on their devices.

#2

The cybercriminals behind this campaign targeted cryptocurrency and stock trading forums. They posed as fellow enthusiasts, sharing trading strategies and linking to modified WinRAR ZIP or RAR archives. These archives appeared to contain trading-related content but contained malware instead. The campaign infected at least 130 traders' devices across eight public trading forums.

#3

When victims opened the archives, they saw what seemed like harmless files alongside folders with matching names. However, double-clicking on these files executed the CVE-2023-38831 vulnerability, launching a script that installed malware. The exploit was designed to appear innocuous, loading the decoy document alongside the malicious script.

#4

The malware strains involved in this campaign included DarkMe, GuLoader, and Remcos RAT. While DarkMe has links to the EvilNum group known for financially motivated attacks, it's not clear if they were responsible for this particular campaign. Remcos RAT provides remote access to infected devices, granting attackers significant control over the compromised system.

#5

This vulnerability was fixed in WinRAR version 6.23, released on August 2, 2023. The fix addressed several security issues, including CVE-2023-40477, which enabled command execution via specially crafted RAR files.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-38831	WinRAR version 6.22 and older versions	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*:*	CWE-20

Recommendations

Upgrade WinRAR: If you use WinRAR, upgrade to the latest version (6.23 or newer) to mitigate the risk associated with CVE-2023-38831 and other potential vulnerabilities.

Update Software Promptly: Ensure that all software, including operating systems and applications, are updated to the latest versions. Regular updates often include security patches that address known vulnerabilities.

Be Cautious Online: Exercise caution when clicking on links or opening email attachments, especially if they're from unfamiliar sources. Cybercriminals often use these tactics to spread malware.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0001 Initial Access	TA0002 Execution	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	T1566.002 Spearphishing Link	T1566 Phishing	T1047 Windows Management Instrumentation
T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059 Command and Scripting Interpreter	T1106 Native API
T1203 Exploitation for Client Execution	T1204.001 Malicious Link	T1204.002 Malicious File	T1204 User Execution
T1559.001 Component Object Model	T1559 Inter-Process Communication	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution
T1055.012 Process Hollowing	T1055 Process Injection	T1548.002 Bypass User Account Control	T1548 Abuse Elevation Control Mechanism
T1574 Hijack Execution Flow	T1027.001 Binary Padding	T1027.003 Steganography	T1027.007 Dynamic API Resolution
T1027.008 Stripped Payloads	T1027.009 Embedded Payloads	T1027 Obfuscated Files or Information	T1036.001 Invalid Code Signature
T1036.006 Space after Filename	T1036.007 Double File Extension	T1055.012 Process Hollowing	T1566.001 Spearphishing Attachment
T1036 Masquerading	T1070.004 File Deletion	T1070 Indicator Removal	T1112 Modify Registry
T1218.011 Rundll32	T1218 System Binary Proxy Execution	T1497.001 System Checks	T1497.002 User Activity Based Checks

T1497.003 Time Based Evasion	T1548.002 Bypass User Account Control	T1548 Abuse Elevation Control Mechanism	T1539 Steal Web Session Cookie
T1555.003 Credentials from Web Browsers	T1555 Credentials from Password Stores	T1606.001 Web Cookies	T1083 File and Directory Discovery
T1573 Encrypted Channel	T1518.001 Security Software Discovery	T1518 Software Discovery	T1056.001 Keylogging
T1056 Input Capture	T1123 Audio Capture	T1115 Clipboard Data	T1113 Screen Capture
T1125 Video Capture	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1090 Proxy
T1105 Ingress Tool Transfer	T1132.002 Non-Standard Encoding	T1571 Non-Standard Port	T1573.002 Asymmetric Cryptography

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1491abddc3885142ff20e1f384587099, c3c578044ff883aac34d8dac65ebd6b2
SHA1	94ea099c591ec582b3edd35f540c1fe0cc954cb4, a0b9d2ea865bc6ad4584f841916d5a66e4ec6259
SHA256	00020783b2b16a30ae8b9ee679bc4c00ed32bad398aadd2ad542c510e3974503, 0059121d725a818e453e29492e78762d0a87087fcb11e484cf5ad663c1eba2bc, 02f9219f9d1bf03b2231f9499780d21b349285601ab8c31be2f5401c479217f2, 05ffced4a39bdbad980daf9ceecc1f6b553ba44a64764645747856c7f1ceb25d, 0860e09e529fc6ccbbffebafedc27497fbbcaff57b5376fb4cc732c331d1f591,

TYPE	VALUE
SHA256	28f1d3b1552529d5e9f706998d441d676a93942fa53c302df6c7b88a4db4b3c6, 296f330696c92bc18982fdd037f93dcf4cd06e012cbd2f883cd8873b9c68c6f8, 2f7c4fd80da91bec3097eeaf62224bd354e9651598f4c007b144aec7345b2364, 32e0fbf08a22602a7cb873b88a90ee35db52c46e0b12cbde85cb1f5bc20e3c98, 379ed799706e5aec25496988ffe391953695094b27583afd243fe72d368005c61, 38d9627f670d63cc2897331fd7bc1241cfdc3696d7c8153d53cfaae79dd18c52, 3d706d77e9982deeda181eb22954a5efcae0534a8202700ec6d17c9af14a597d, 3e8e4a10ee7ca9e99f3c243acd058d5544dfde64fcfc8224d59c27fab51edbea, 414d2acaf75f70773cdd4c11684a50c123f4ba7643fd90732c181d9cceb4e53f, 416b6abe887886a1be22a7a234ad19d4aaaf50a3bbe64a4bc2f65872dd3c9330, 43f5eb815eed859395614a61251797aa777bfb694a9ef42fbafe058dff84d158, 48798522aaf20bb629639741b645e5e12bddf18763f983259097030362c2c337, 52193f1d50beab7f07ff712001b711d701bc9454ec6ce661118e206f0f41b619, 53a77813c5730067f42158767d499efa49b3dccede6820d4ab90d3e6c6772ff2, 5a387ee6d0dcbbf2cd97379c68d8e3398d01a920873ddd45ff21dbfccb19e2ee, 61c15d6a247fbb07c9dcbce79285f7f4fcc45f806521e86a2fc252a311834670, 61f88c557364657bfa12e1f145cc53d186686ac503b30b55c74d5e9020b64d95, 6ecf38e5fb7e583999c558e837e8dfa23d2113d623377892349a03176389d154, 721d29ab70e0bae72ab29228c007bc29a128a7eaee80a83d4b3e32a04356f4ec, 7563473bb8e3621fc5376e790bb55b6ae72070430e2816dd5841c679035bf27b, 763df8b2db7f2f2fa0c8adb8c1cc05ff15b59e6a9756cbe9fc4a1c12329b62af, 80dc3c6054c161e5de38cd0833934ab6aa3c9546c382004978462e30006fc564, 896987527a9e25e4cce765dd5309bdf81ea25b9db024aba585b4c2c320679f51, 8993384715f59636fb4c59ba70db3214c56a9314c8eff7d23f3a9e126c790347,

TYPE	VALUE
SHA256	8deebfe4685c9f79be484e10f9db886370d22ba0883467a3671e58825de503b0, a2e3aae8805fad2b3062d8ef35341b6c47fe91e531bc015d0be783715dbb0599, a3d684e52c893e64b30473ed408bd33ea8cdbec3f05df43edcea9489f3551d55, ac9d88036a60b6aaa7e32b88c3e7dd551075e9709d4c77681329feca138b2927, aea3fd161b49c4002d117e37c4119f3759cea23c0368c48d04949704f80aebaa, af84d48c63c8e4fd5b097b7529ef878f7b708d4ec1d7d1be1c449771be2b75aa, b27b5877e91ea876a40949d1aa3c0db634b9dcc1a2867bfcc29448c10a5a75a8, b3d1f7b162f2efee3d94eabb6a4cd2d331f42ef964d999dd8080dbae94c8aa2a, bc15b0264244339c002f83e639c328367efb1d7de1b3b7c483a2e2558b115eaa, bfb8ca50a455f2cd8cf7bd2486bf8baa950779b58a7eab69b0c151509d157578, c350f7f29878fac639b93831dad33b2606abc1a28deec2a1c2d4f3c26823cc19, c620ba7b6dfe81c6b6bf54a3e6a98bbca7b77e0c3f75586b900af326b8fd7cfe, c7f932111eb3adc6f6efe7a157209eb72c6bcd8ce172d5ce086feb5d01d73c80, ccbab5637206b2045816bad1da6738779d14da48f5009bfe0781605a49b18035, db9b74c07e05b834c064226253bea88b8e439af12ac42613af0de012d552ff53, e29267b51f74e42574739a8a0b18630cc5b960a8a8c036587e5fc97a0a51af63, e7684d1cb5b6751c9b47aface25e0f3aa50d87b33815f76ca3f2c3025e1745bb, ead3ba2e04035d60416375d1dc0b28ae59224885fd715b38e941f720cf3a23df, ee7a36e3cdeb1a96908f4ac1c4cc700c95d62491ad6a2fffc0997ce40bfe7638, ef23bd825c60db487c8b29e97607c853d180ccc2109ce13f1675a5519dff58a2, f136777d0600495844b0662984fdaa4d9e1cbfd72bc08318ed639c2935df62a6, f6d77a353146d212a6b71fdbc387effbfbd3eb964a431701a228e2f731905199, f7cc87cf6909c320cb578de5ff6a7129dbc65c2541aab325f9577e4090c8abe9, f90dbad9711c7bafc7b4ab9158837fb3ad0b434771f35d45946d04afb26bd013, fea41cb849d7c4b1a0cbb349e7b83cd9db8ac6eeeba56287e6cde720cf82c402,

TYPE	VALUE
SHA256	0a82c4e3778e21a8592142ca1643d95f4520495eff47d43964dc8680de9113ad, 11a42cebf171bab62dfad87536bcbaf9fcf84aa7c69705f40e106214d175d2c5, 15cd319826ca545a40dc369c81a740b1472e87fd9b4dd197b0ab8bee294ebcac, 16a95486b8c0e22035f5b127c03dd2313c63f9058fbe74f81af7ed9292beb642, 18129626041b90558607eec67616ba6d2b1ea28a280c7ba5b2bd30ebb1e2438b, 1a0d604c3e6e8298edb08e35df725441b14d2f50a4ae554cb58f45eea6dc95d8, 1a87678b77d45ad38968578e8edf6720bd9a0c6ebc771f1ad507e7878e326bbe, 1b85a05b96aafd4b201c7bea4330b59c8d8e1375b3d9feb3cf0ee087f05a7814, 1fdac9c692503bd9c6d54de8d663e7934175b368ed333b9ec79f46ee94cb46d1, 2010a748827129b926cf3e604b02aa77f5a7482da2a15350504d252ee13c823b, 20e31ce447d5368cec1c874ebcefdcf1dc61d64dc9b836740850737751d69d4c, 2169065ee6159aea5fc0216a205a9ca43a64fc3ea9bd0f8cf2ad3e8b03f85dd8, 23ebe986f64ebefd87e628bfe5efb5f41bade0ee8e9c71df2cec0e510b21eb24, 25f28bc9532514db37ed4b39dea9df3581809f3f66013dff68685d284ea7bf47, 27814283a47a02556cb43c3881b3dc5f14b7664b9ad21cfe8c9120ecfa347697
IPv4	153.92.126.196, 45.74.19.105, 45.74.19.87, 45.74.19.89, 45.74.19.96, 51.195.57.234, 91.148.135.198
Domains	12jyyu06.com, 87iavv.com, corialopolova.com, images.com, mmnedgeggrrva.com, tganngs9.com, trssp05923.com, weakicons.com

Patch Details

Update WinRAR version to 6.23 or later versions

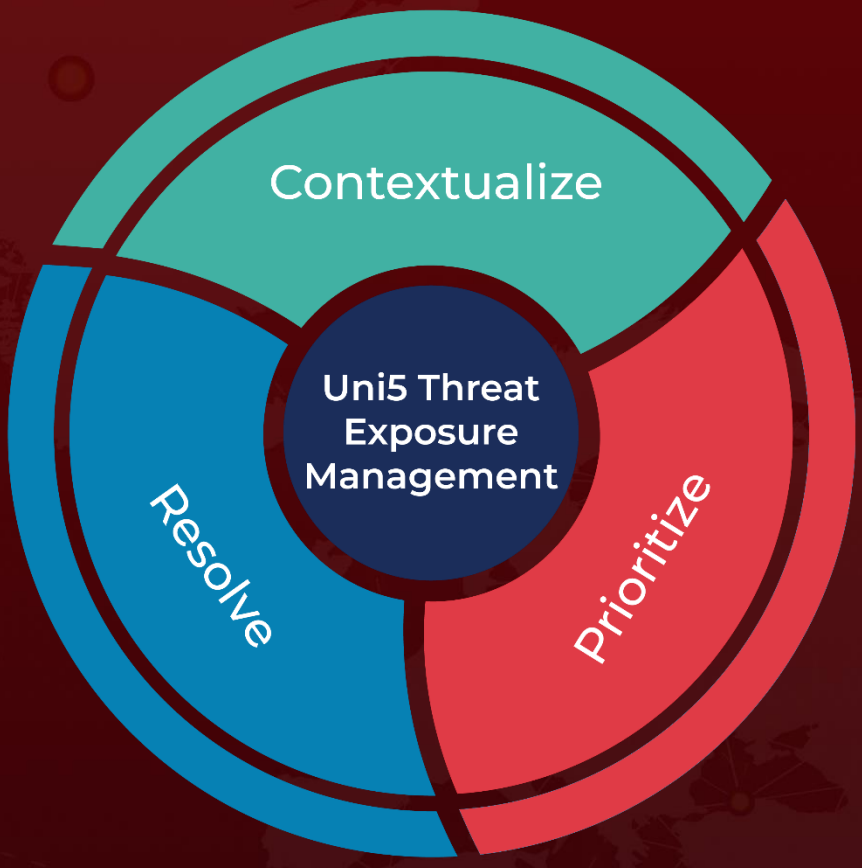
References

https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/

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 24, 2023 • 7:00 AM

More at www.hivepro.com