Government-backed actors exploiting WinRAR vulnerability

Kate Morgan

October 18, 2023

Threat Analysis Group

In recent weeks, Google's Threat Analysis Group's (TAG) has observed multiple government-backed hacking groups exploiting the known vulnerability, CVE-2023-38831, in WinRAR, which is a popular file archiver tool for Windows. Cybercrime groups began exploiting the vulnerability in early 2023, when the bug was still unknown to defenders. A patch is now available, but many users still seem to be vulnerable. TAG has observed government-backed actors from a number of countries exploiting the WinRAR vulnerability as part of their operations.

To ensure protection, we urge organizations and users to keep software fully up-to-date and to install security updates as soon as they become available. After a vulnerability has been patched, malicious actors will continue to rely on n-days and use slow patching rates to their advantage. We also recommend use of Google's Safe Browsing and Gmail, which block files containing the exploit.

Patch and proof-of-concept

In August 2023, RARLabs released an updated version of WinRAR that included fixes for several security-related bugs. One of those bugs, later assigned CVE-2023-38831, is a logical vulnerability within WinRAR causing extraneous temporary file expansion when processing crafted archives, combined with a quirk in the implementation of Windows' ShellExecute when attempting to open a file with an extension containing spaces. The vulnerability allows attackers to execute arbitrary code when a user attempts to view a benign file (such as an ordinary PNG file) within a ZIP archive.

As detailed in a blog post from Group-IB, the vulnerability had been exploited as 0-day by cybercrime actors in-the-wild since at least April 2023 for campaigns targeting financial traders to deliver various commodity malware families. Hours after the blog post was released, proof of concepts and exploit generators were uploaded to public GitHub repositories. Shortly after that, TAG began to observe testing activity from both financially motivated and APT actors experimenting with CVE-2023-38831.

Vulnerability

Consider the following archive structure:

a picture of code

When a user double-clicks on a benign “poc.png_” (underscore is used to indicate a space) from WinRAR’s user interface, WinRAR prior to 6.23 will instead execute “poc.png_/poc.png_.cmd”.

After a user double-clicks on a file, WinRAR attempts to determine which files need to be temporarily expanded by iterating through all archive entries. However, due to the way the matching is made, if a directory is found with the same name as the selected entry, both the selected file and the files inside a matched directory are extracted to the root of a random temporary directory.

The pseudocode below shows WinRAR’s extraction logic and whether an archive entry should to be extracted:

a picture of code

When writing contents of the files, WinRAR performs path normalization that removes appended spaces, because Windows doesn’t allow files with trailing spaces.

Finally, WinRAR calls ShellExecuteExW, passing the non-normalized path with a trailing space “%TEMP%\{random_directory}\poc.png_” to run the user-selected file. Internally, ShellExecute attempts to identify file extensions by calling “shell32!PathFindExtension” which fails because extensions with spaces are considered invalid. Instead of bailing out, ShellExecute proceeds to call “shell32!ApplyDefaultExts” which iterates through all files in a directory, finding and executing the first file with an extension matching any of the hardcoded ones: “.pif, .com, .exe, .bat, .lnk, .cmd”.

Note, that while most samples exploiting CVE-2023-3883 use an archive entry with a trailing space, it is not a requirement, and a space in any position in the file extension is sufficient to trigger the bug (e.g. entry with “poc.invalid_ext” will also result in “shell32!ApplyDefaultExts” code path to be taken).

a box showing lines of code

This quirk in ShellExecute, causing the default extension search logic to be applied when attempting to open a file with an extension containing spaces is what causes “poc.png_.cmd” to be selected and inadvertently run, even though it was not the file the user originally double-clicked on.

Campaigns

FROZENBARENTS impersonates Ukrainian drone training school to deliver Rhadamanthys infostealer

In a blog post earlier this year, TAG reported on FROZENBARENTS (aka SANDWORM) targeting the energy sector and continuing hack & leak operations. The group, attributed to Russian Armed Forces' Main Directorate of the General Staff (GRU) Unit 74455, on September 6th launched an email campaign impersonating a Ukrainian drone warfare training school.

Using a lure themed as an invitation to join the school, the email contained a link to an anonymous file-sharing service, fex[.]net, which delivered a benign decoy PDF document with a drone operator training curriculum and a malicious ZIP file exploiting CVE-2023-38831 titled "Навчальна-програма-Оператори.zip" (Training program operators).

a decoy document with letters
"Training of drone operators" decoy document from FROZENBARENTS campaign

The payload, found in "Навчальна-програма-Оператори.pdf /Навчальна-програма-Оператори.pdf_.bat" was a packed Rhadamanthys infostealer. Rhadamanthys is a commodity infostealer that is able to collect and exfiltrate browser credentials and session information among other things. It operates on a subscription-based model and can be rented out for as low as $250 for 30 days. Usage of commercially available infostealers, that are typically employed by cybercrime actors, is atypical of FROZENBARENTS.

FROZENLAKE spear-phishing campaign targeting Ukrainian government organizations hosted on API endpoint testing services

On September 4th, CERT-UA posted about FROZENLAKE (aka APT28), a group attributed to Russian GRU, using CVE-2023-38831 to deliver malware targeting energy infrastructure. TAG observed that FROZENLAKE used a free hosting provider to serve CVE-2023-38831 to target users in Ukraine. The initial page redirected users to a mockbin site to perform browser checks and redirect to the next stage, which would ensure the visitor was coming from an IPv4 address in Ukraine and would prompt the user to download a file containing a CVE-2023-38831 exploit. The decoy document was an event invitation from Razumkov Centre, a public policy think tank in Ukraine.

a decoy document from the Frozenlake campaign
FROZENLAKE decoy document impersonating a Ukrainian public policy think tank

FROZENLAKE using IRONJAW with reverse SSH shell

A sample with a filename "IOC_09_11.rar" (072afea7cae714b44c24c16308da0ef0e5aab36b7a601b310d12f8b925f359e7) was uploaded to VirusTotal on September 11th. The sample exploits CVE-2023-38831 to drop a

BAT file which opens a decoy PDF file and creates a reverse SSH shell to an attacker controlled IP address, and executes IRONJAW script using PowerShell.

box showing code

IRONJAW is a small PowerShell script that steals browser login data and local state directories, exfiltrating them to a C2 on “http://webhook[.]site/e2831741-d8c8-4971-9464-e52d34f9d611”. IRONJAW was first observed being distributed by ISO files hosted on free hosting providers in late July through early August and attributed to FROZENLAKE. The additional delivery of IRONJAW via exploitation of CVE-2023-38831 and the reverse SSH tunnel were new additions to the typical FROZENLAKE toolkit.

ISLANDDREAMS delivering BOXRAT in campaign targeting Papua New Guinea

TAG has also observed government-backed groups linked to China exploit CVE-2023-38831. In late August, ISLANDDREAMS (aka APT40) launched a phishing campaign targeting Papua New Guinea. The phishing emails included a Dropbox link to a ZIP archive containing the CVE-2023-38831 exploit, a password-protected decoy PDF, and an LNK file.

decoy PDF reading "password required"

Decoy PDF used in ISLANDDREAMS campaign

The next stage payload, ISLANDSTAGER, is either an XOR-encoded DLL found at a hardcoded offset inside of the LNK, or downloaded from a hardcoded URL of a file-sharing service.

black box showing lines of code

ISLANDSTAGER is then executed by starting a legit “ImagingDevices.exe” process which sideloads malicious “STI.dll” from “%ProgramData%\Microsoft\DeviceSync\”. ISLANDSTAGER configures persistence by adding “ImagingDevices.exe” to “CurrentVersion\Run” registry key. It then decodes several layers of shellcode, the last of which is generated using Donut, that loads and executes the final payload, BOXRAT, in-memory. BOXRAT is a .NET backdoor that uses Dropbox API as a C2 mechanism.

Conclusion

The widespread exploitation of the WinRAR bug highlights that exploits for known vulnerabilities can be highly effective, despite a patch being available. Even the most sophisticated attackers will only do what is necessary to accomplish their goals. These recent campaigns exploiting the WinRAR bug underscore the importance of patching and that there is still work to be done to make it easy for users to keep their software secure and up-to-date. TAG will continue to compile and share threat intelligence for the protection of online users and Google products, in the meantime, we encourage organizations and users to keep their software fully up-to-date.

Indicators of compromise (IoCs)

FROZENBARENTS

- https://fex[.]net/s/bttyrz4
- https://fex[.]net/s/59znp5b

FROZENLAKE

- 072afea7cae714b44c24c16308da0ef0e5aab36b7a601b310d12f8b925f359e7
- 91dec1160f3185cec4cb70fee0037ce3a62497e830330e9ddc2898f45682f63a
- 77cf5efde721c1ff598eeae5cb3d81015d45a74d9ed885ba48330f37673bc799
- 216.66.35[.]145
- http://webhook[.]site/e2831741-d8c8-4971-9464-e52d34f9d611

ISLANDDREAMS

https://filetransfer[.]io/data-package/DVagoJxL/download

POSTED IN:

Threat Analysis Group

Related stories

- Threat Analysis Group

  TAG Bulletin: Q4 2023

  This bulletin includes coordinated influence operation campaigns terminated on our platforms in Q4 2023. It was last updated on December 15, 2023.OctoberWe terminated 8 …

  By Shane Huntley

  Dec 15, 2023

-

  Threat Analysis Group

  Zimbra 0-day used to target international government organizations

  By Clement Lecigne Maddie Stone

  Nov 16, 2023
- Threat Analysis Group

  TAG Bulletin: Q3 2023

  This bulletin includes coordinated influence operation campaigns terminated on our platforms in Q3 2023. It was last updated on November 8, 2023.

  By Shane Huntley

  Oct 05, 2023
- Threat Analysis Group

  0-days exploited by commercial surveillance vendor in Egypt

  Last week Google’s Threat Analysis Group (TAG), in partnership with The Citizen Lab, discovered an in-the-wild 0-day exploit chain for iPhones. Developed by the commerci…

  By Maddie Stone

  Sep 22, 2023

- Threat Analysis Group
  Active North Korean campaign targeting security researchers

  Threat Analysis Group shares findings on a new campaign by North Korean actors targeting security researchers.

  By Clement Lecigne Maddie Stone

  Sep 07, 2023
- Threat Analysis Group
  TAG Bulletin: Q2 2023

  Threat Analysis Group shares their Q2 2023 bulletin.

  By Shane Huntley

  Jul 31, 2023
- .