Discovering and Blocking a Zero-Day Exploit with CrowdStrike Falcon Complete: The Case of CVE-2023-36874

August 10, 2023 | Nicolas Zilio - Ken Balint - Marco Ortisi | Counter Adversary Operations

CrowdStrike Counter Adversary Operations is committed to analyzing active exploitation campaigns and detecting and blocking zero-days to protect our customers. In July 2023, the CrowdStrike Falcon® Complete managed detection and response (MDR) team discovered an unknown exploit kit leveraging a still-unknown vulnerability affecting the Windows Error Reporting (WER) component. Our team prepared to report this newly discovered vulnerability to Microsoft — only to discover that the Google Threat Analysis Group had independently discovered and disclosed it shortly before we did. Microsoft assigned the identifier CVE-2023-36874 to the vulnerability.

Given this vulnerability was a zero-day when Falcon Complete found it, we are sharing the story of how our team discovered this issue, as well as technical details and some indicators of compromise. ***The CrowdStrike Falcon® platform protects against exploitation of CVE-2023-36874.***

The Story

On June 22, 2023, Falcon Complete observed multiple binaries being dropped onto a system owned by a European technology entity via Remote Desktop Protocol (RDP) connection from an unmanaged host. The Falcon sensor

CATEGORIES

- Cloud & Application Security 104
- Counter Adversary Operations 184
- Endpoint Security & XDR 307
- Engineering & Tech 78
- Executive Viewpoint 162
- Exposure Management 84
- From The Front Lines 190
- Identity Protection 37
- Next-Gen SIEM & Log Management 91
- Public Sector 37
- Small Business 8

CONNECT WITH US

correct potential vulnerability used. The results indicated the use of an unknown vulnerability affecting the WER component. Hence, at the time of execution, Falcon Complete detected a still-unknown zero-day in the wild, along with an exploit kit using it.

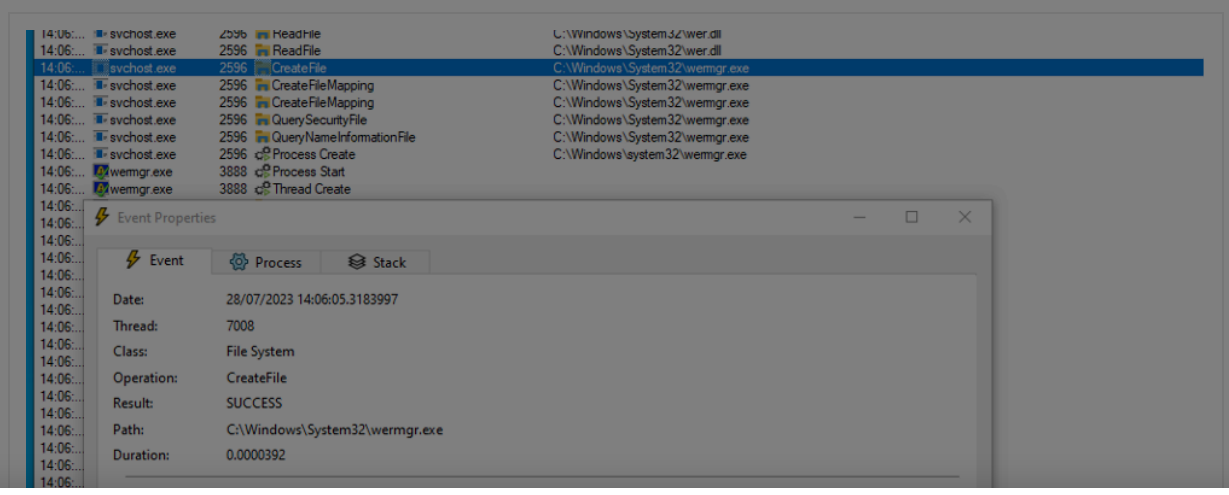
The Technical Details

The WER service is a privileged service whose role is to analyze and report various software issues that may arise on a Windows host. This service can be interacted with through several undocumented COM interfaces, which can be found in `wercplsupport.dll`. In particular, by chaining the following function calls, it is possible to get a pointer to a `IWerReport` COM interface:

1. `CoCreateInstance(CLSID_ERCLuaSupport, NULL, CLSCTX_LOCAL_SERVER, IID_IErcLuaSupport, (PVOID*)&pIErcLuaSupport);`
2. `pIErcLuaSupport->CoCreateIWerStoreFactory(&pIWerStoreFactory);`
3. `pIWerStoreFactory->CoCreateIWerStore(&pIWerStore);`
4. `pIWerStore->EnumerateStart()`
5. `pIWerStore->LoadReport(<reportName>, &pIWerReport);` where reportName is the name of a directory containing a WER report to be processed

As a result of calling `IWerReport->SubmitReport`, the WER service will call the `WerpSubmitReportFromStore` function from `wer.dll`. This eventually leads, under conditions that were not analyzed, to the call of the `UtilLaunchWerManager` function, itself calling the `CreateProcess` API in order to start the `C:\Windows\System32\wermgr.exe` executable.

The core problem of this vulnerability lies in the fact that the CreateProcess API running under impersonation will follow any file system redirection set up by a threat actor but will use the calling process security token and not the impersonated token to set the security context of the process. In the case of the WER service, impersonation is indeed present when the `wermgr` process creation occurs, as highlighted in the following screenshot:



September 25, 2024

Recognizing the Resilience of the CrowdStrike Community
September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection
September 18, 2024

In the case of the observed exploit, the following steps are taken to achieve privilege escalation:

1. The exploit sets up the necessary files on the system to achieve successful exploitation later. Two different objectives are followed at this step:
    a. Set up a dummy `Report.wer` file in the directory `C:\ProgramData\Microsoft\Windows\WER\ReportArchive\WER1CF4123`. This dummy file will be referenced in the `IWerReport->SubmitReport` function at the start of the exploit chain.
    b. Set up a fake `C:\` root hierarchy under the `C:\Users\public\test` directory so the file system redirection will point to the attacker files instead of the legitimate ones. In this hierarchy, the exploit creates a copy of itself as `C:\Users\public\test\Windows\System32\wermgr.exe` as well as a dummy WER report `Report.wer` inside `C:\Users\Public\test\ProgramData\Microsoft\Windows\WER\ReportArchive\WER1CF4123`.
2. Creates a redirection from the `C:\` drive to `C:\Users\public\test` by calling the `NtCreateSymbolicLink` function, where the third and fourth parameters point respectively to `\??\C:` and `\GLOBAL??\C:\Users\Public\Test`. This redirection is created when changes are detected in the `C:\\ProgramData\\Microsoft\\Windows\\WER\\ReportQueue` directory.
3. Triggers `IWerReport->LoadReport()` with `WER1CF4123` as a parameter.
4. Triggers `IWerReport->SubmitReport()` with `WER1CF4123` as a parameter.
5. Due to redirection, `C:\Users\public\test\Windows\System32\wermgr.exe` is executed instead of the legitimate `wermgr.exe`. The exploit binary is now executing with high privileges.

A Look at the Exploit Kit

In the exploit kit observed, all exploit binaries aim to spawn a privileged interpreter, either the traditional command interpreter `cmd.exe`, or `powershell_ise.exe`, in the interactive session from which the binary was launched. If this aim cannot be fulfilled, then a privileged scheduled task is created to serve as a proxy for the spawning of the privileged interpreter.

Within the exploit kit observed, some binaries are packed while others are not.

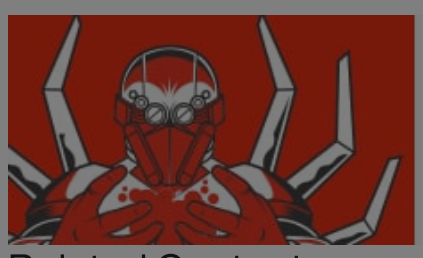
dropped. It should be noted the following indicators are of low fidelity. Indeed, several of them are packed, indicating the threat actor has the potential capability to generate new binaries, with different hashes, containing the exploit.

Filename	SHA256 Has
10new+11_ISE_0x000109D59D6CC3F4.exe	e800d1271b
8_ise.exe	338ac127e8
8.exe	15b9f28271
2019_ise.exe	11243b8c4c
2019.exe	69411eebef
2016_ise.exe	7de0700837
2016.exe	5251fb2f99
WER_Research_07062023_ise_0x00000F0B67DB1762.exe	7251149fe9
10new+11.exe	1efd500697
8_0x000109ABFE57D295.exe	06d1a07529
2019_0x000109ED1C1A33D9.exe	ed6e026059
10_ISE_0x000109C422FAC8CA.exe	84ea56d15e
WER_Research_07062023_cmd_0x00000EF75A5B64F2.exe	130f0a4293
10new+11_ise.exe	80185c0c10
10_0x000109BCF309A283.exe	06be6b9b71
2016_0x000109DC78E96163.exe	96f0546ac6
2019_ISE_0x000109F402AB3D7F.exe	0c19f42339
8_ISE_0x000109B5EDC3E0B1.exe	5fe77c71b7
10.exe	43f3a7a530
10_ise.exe	1b3ee2bbb3

Conclusion

Additional Resources

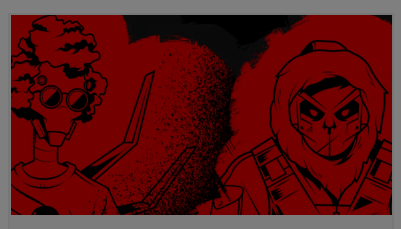
- *Learn more about today's adversaries and how to combat them at Fal.Con 2023, the can't-miss cybersecurity experience of the year. Register now and meet us in Las Vegas, Sept. 18-21!*
- *Know the adversaries that may be targeting your region or business sector — explore the CrowdStrike Adversary Universe.*
- *Request a free CrowdStrike Intelligence threat briefing and learn how to stop adversaries targeting your organization.*
- *Watch an introductory video on the CrowdStrike Falcon console and register for an on-demand demo of the market-leading CrowdStrike Falcon platform in action.*



Related Content

U.S. Department of Justice Indicts Hacktivist Group Anonymous Sudan for Prominent DDoS Attacks in 2023 and 2024

International Authorities Indict, Sanction Additional INDRIK SPIDER Members and Detail Ties to BITWISE SPIDER and Russian State Activity



How CrowdStrike Hunts, Identifies and Defeats Cloud-Focused Threats

« CrowdStrike Debuts Counter Adversary Operations Team to Fight Faster and Smarter

Amid Sharp Increase in Identity-Based Attacks, CrowdStrike Unveils New Threat Hunting Capability

ABOUT COOKIES ON THIS SITE

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**