Falcon Complete: Zero-Day Exploit Case Study

crowdstrike.com/blog/falcon-complete-zero-day-exploit-cve-2023-36874/

Nicolas Zilio - Ken Balint - Marco Ortisi

August 10, 2023

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 blocked and quarantined the execution of several of these binaries as it detected potential exploits for CVE-2021-24084. An initial analysis by the Falcon Complete team was conducted to determine the final objectives of these binaries; however, it was inconclusive. CrowdStrike Counter Adversary Operations was asked to assist, given the team's expertise in both threat hunting and adversary intelligence, in order to accelerate the detection and remediation of threats.

During the first static analysis of these binaries, a string containing the Russian word 0дэй — translated as "0day" — indicated the binaries may be exploits related to an unknown vulnerability. A thorough analysis ensued to pinpoint the 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.

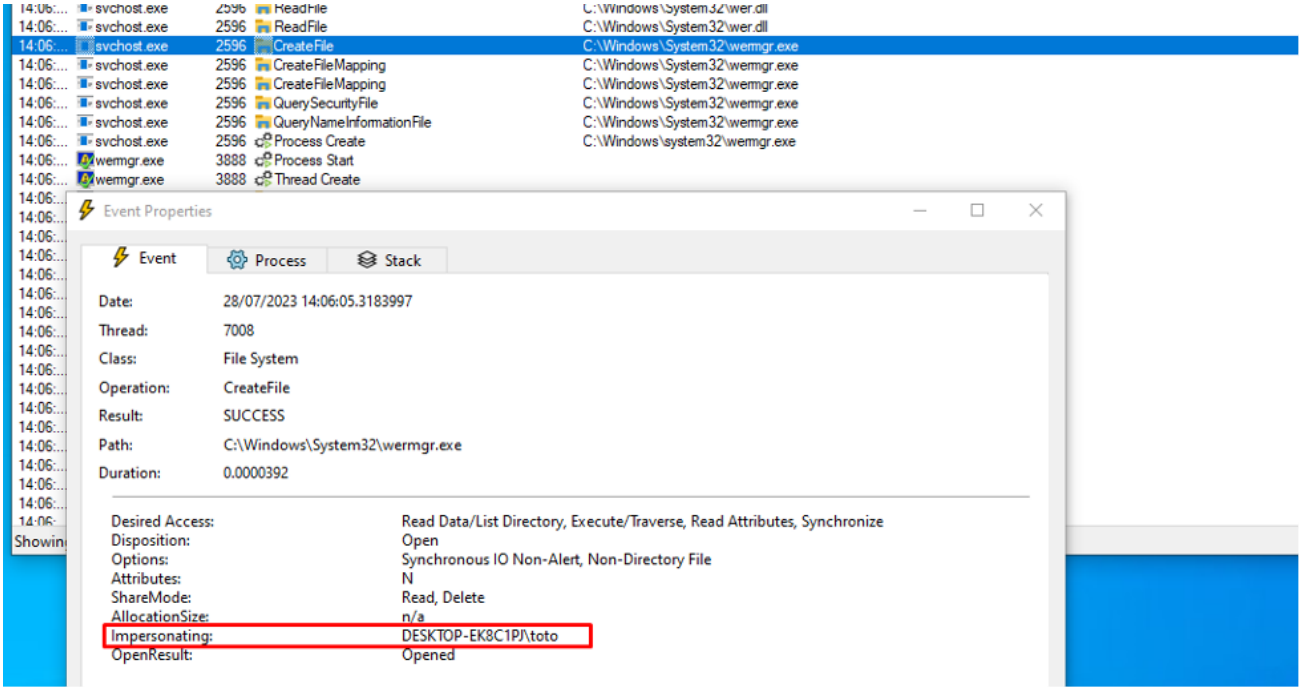
The Technical Details

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:



Click to enlarge

This means, in the case a prior file system redirection points to an attacker-controlled `wermgr` executable, this executable will be executed instead of the legitimate `wermgr` executable. This allows the attacker-controlled executable to be run with the privileges of the WER service (i.e., SYSTEM).

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:
    1. 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.
    2. 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. Some contain C++ code while others appear to be pure C code. Some binaries were apparently able to launch multiple versions of the same exploit depending on the host's OS version while others appear dedicated to a single OS. This information tends to indicate that the privilege escalation vulnerability was likely known to a group of different developers.

At the time of this writing, CrowdStrike Counter Adversary Operations does not attribute the activity to a particular actor.

Indicators of Compromise

The following table lists the different binaries that CrowdStrike observed being 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 Hash
10new+11_ISE_0x000109D59D6CC3F4.exe	e800d1271b15d1db04280a64905104a912094d2938fd6b024ce143f1221d22f5
8_ise.exe	338ac127e81316d3b4a625ddf28eff2693778f3c8f1050cc06467845232e8da2
8.exe	15b9f282717b6539e44a7a5e0ceafaae1eff09cadfbf46982e4d7e78a605cf3c
2019_ise.exe	11243b8c4da386fed7efd500076f5671f649c25b7edb90416ec91b3e4a2073a5
2019.exe	69411eebef102e63d86bd3e88c363375934ed9dee94ca9342b694c4be232c792
2016_ise.exe	7de07008373bacf77ce9079c2374dd87afaa605b857b8ab440661faa0ca7d504
2016.exe	5251fb2f9979dbc21b83e6e770c767595848ad9b01c94713683613a6d8561561
WER_Research_07062023_ise_0x00000F0B67DB1762.exe	7251149fe93811b5b1a84418d0fe07296469c34b57f70f9107e0b9a1726b1080
10new+11.exe	1efd5006979b10c60eefc367f529799b7b9dd2be1162e0195b22eedde32b7f7b
8_0x000109ABFE57D295.exe	06d1a0752960576051ae5845d2ec38154a33b5de36ed268d61da26574bba3368
2019_0x000109ED1C1A33D9.exe	ed6e026059653e3b6d05a479ad27c1b38f790a840bcef38f1a06a73ff476525d
10_ISE_0x000109C422FAC8CA.exe	84ea56d15ebb895b1688339fb230e2b9b61b35389cc7ea8dedbd2f92bb92ab10
WER_Research_07062023_cmd_0x00000EF75A5B64F2.exe	130f0a4293fb842d99d2044d449e3320de8add982177ed1ad03ba0fef9bcf096
10new+11_ise.exe	80185c0c10a4046fd4ca1242ccbd63bef7765c6e93a3f53c90107d34e0d790fe
10_0x000109BCF309A283.exe	06be6b9b7163489854864292f9516558f6e192dda01560ea772fbc82dc1471df
2016_0x000109DC78E96163.exe	96f0546ac6c722576f860f9a23d35fd93a8df1c547bd92d0836bb845cc875002
2019_ISE_0x000109F402AB3D7F.exe	0c19f42339735cdd9d6a4c55e2f8f93b9d559d7a3420557487a75f67a2a946c0
8_ISE_0x000109B5EDC3E0B1.exe	5fe77c71b75b71d95f2d62c71f3054afce1f3026873d107a9a56d701c503c2d7
10.exe	43f3a7a5300fa89b7b9783cf97ca3a5f9d1f45535e71a80ac2b8b16d21a64fe8
10_ise.exe	1b3ee2bbb3baff96e3637b0ee3ad5831c9c7741db7a32411281d0bcd4f26f012

Conclusion

It is critical to ensure timely vulnerability patching in order to protect enterprise devices. However, when adversaries target unknown vulnerabilities, timely patching becomes irrelevant. This is why it's essential for organizations to implement multiple layers of defense such as CrowdStrike Falcon Complete managed detection and response. The Falcon Complete team actively monitors for, and remediates, vulnerabilities such as CVE-2023-36874 so organizations have 24/7 protection from the latest threats — including zero-days exploited in the wild.

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.*