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

Featured
Recent
Video
Category
Start Free Trial

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.***

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

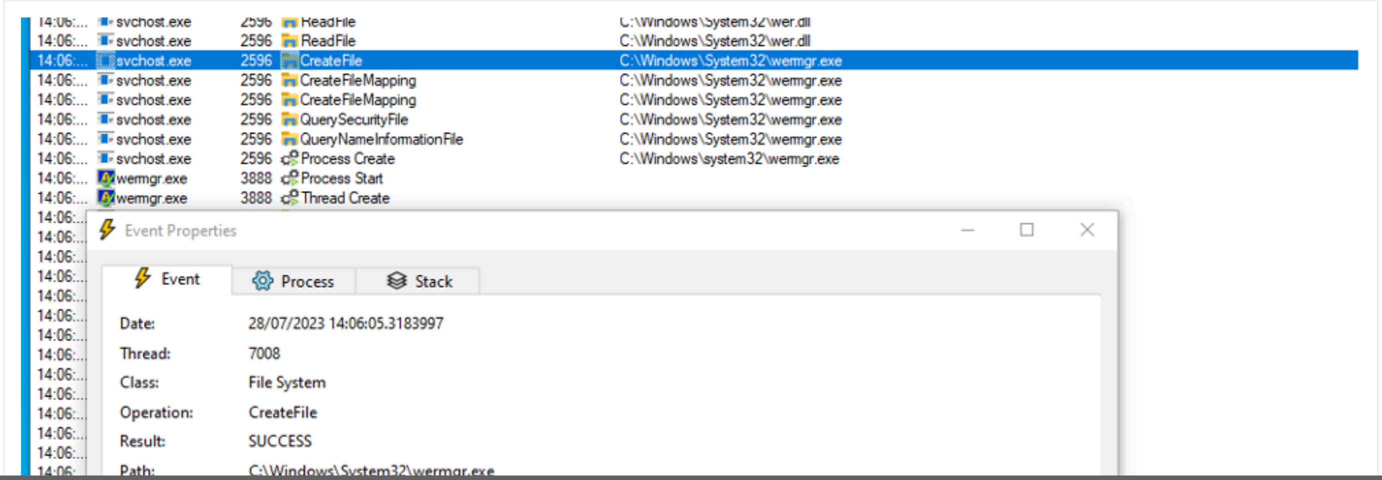
The WER service is a privileged service whose role is to analyze and report various software issues that may arise on a Windows host. This service can be interacted with

Featured
Recent
Video
Category
Start Free Trial

3. `pIWerStoreFactory->CoCreateIWerStore(&pIWerStore);`
4. `pIWerStore->EnumerateStart()`

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:



```
14:06:...  svchost.exe  2596  ReadFile                  C:\Windows\System32\wer.dll
14:06:...  svchost.exe  2596  ReadFile                  C:\Windows\System32\wer.dll
14:06:...  svchost.exe  2596  CreateFile                C:\Windows\System32\wermgr.exe
14:06:...  svchost.exe  2596  CreateFileMapping         C:\Windows\System32\wermgr.exe
14:06:...  svchost.exe  2596  CreateFileMapping         C:\Windows\System32\wermgr.exe
14:06:...  svchost.exe  2596  QuerySecurityFile         C:\Windows\System32\wermgr.exe
14:06:...  svchost.exe  2596  QueryNameInformationFile  C:\Windows\System32\wermgr.exe
14:06:...  svchost.exe  2596  Process Create            C:\Windows\system32\wermgr.exe
14:06:...  wermgr.exe   3888  Process Start
14:06:...  wermgr.exe   3888  Thread Create
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
14:06:...
```

```
Date:       28/07/2023 14:06:05.3183997
Thread:     7008
Class:      File System
Operation:  CreateFile
Result:     SUCCESS
Path:       C:\Windows\System32\wermgr.exe
```

Featured
Recent
Video
Category
Start Free Trial

`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).

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.

Featured
Recent
Video
Category
Start Free Trial

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

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	e800d1271b15d1db04
8_ise.exe	338ac127e81316d3b4
2016_ise.exe	[illegible]
2016.exe	5251fb2f9979dbc21b

10new+11.exe	1efd3006979b10c60e
8_0x000109ABFE57D295.exe	06d1a0752960576051
2019_0x000109ED1C1A33D9.exe	ed6e026059653e3b6c
10_ISE_0x000109C422FAC8CA.exe	84ea56d15ebb895b16
WER_Research_07062023_cmd_0x00000EF75A5B64F2.exe	130f0a4293fb842d99
10new+11_ise.exe	80185c0c10a4046fd4
10_0x000109BCF309A283.exe	06be6b9b7163489854
2016_0x000109DC78E96163.exe	96f0546ac6c722576f
2019_ISE_0x000109F402AB3D7F.exe	0c19f42339735cdd9c
8_ISE_0x000109B5EDC3E0B1.exe	5fe77c71b75b71d95f
10.exe	43f3a7a5300fa89b7b
10_ise.exe	1b3ee2bbb3baff96e3

Featured
Recent
Video
Category
Start Free Trial

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.

- *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.*

Tweet Share

Related Content

Featured
Recent
Video
Category
Start Free Trial

Anonymous Sudan for Prominent DDoS

Additional INDRIK SPIDER Members and Detail Ties to

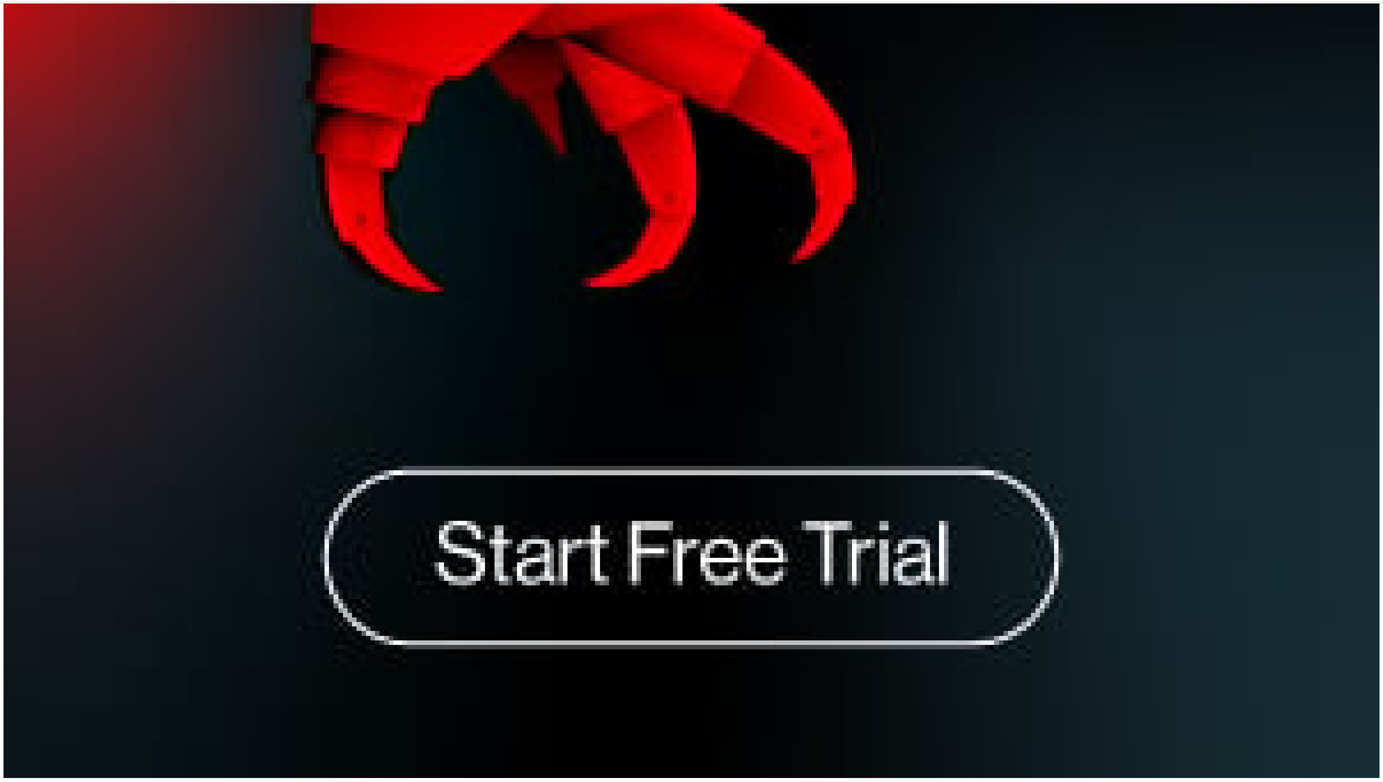
and Defeats Cloud-Focused Threats

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

Featured
Recent
Video
Category
Start Free Trial

Featured
Recent
Video
Category
Start Free Trial


Start Free Trial

CROWDSTRIKE | BLOG

October 01, 2024

CrowdStrike Named a Leader in 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

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

Featured

Recent

Video

Category

Start Free Trial

« CrowdStrike Debuts Counter Adversary Operations Team to Fight Faster and Smarter Adversaries as Identity-Focused Attacks Skyrocket

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