Windows Event Log - Audit-CVE

Mike
Jan 18, 2020 • 2 min read

Update: This event appears for both binaries and websites in build 1809 and 1909, but only for binaries in 1903 (not web). So if you're looking for this event and not finding it, that may be why. I have not confirmed this myself, so if someone else comes across this, please let me know in the comments.

Some of you may have heard by now that there's a new Microsoft EVTX log going around. In this particular case, it detects attempted exploitation of CVE-2020–0601. Ideally, this source, "Microsoft-Windows-Audit-CVE" could be used to detect the attempted (or actual) exploitation of any other vulnerability in the future. Here's what it looks like right now:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Audit-CVE" Guid="{85a62a0d-7e17-485f-9d4f-749a287193
  <EventID>1</EventID>
  <Version>0</Version>
  <Level>3</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000000000</Keywords>
  <TimeCreated SystemTime="2020-01-18T18:14:29.831868400Z" />
```

```
    <EventRecordID>19156</EventRecordID>
    <Correlation />
    <Execution ProcessID="23004" ThreadID="22388" />
    <Channel>Application</Channel>
    <Computer>Isaac</Computer>
    <Security UserID="S-1-5-21-955638165-4017457581-270078328-1001" />
    </System>
  - <EventData>
    <Data Name="CVEID">[CVE-2020-0601] cert validation</Data>
    <Data Name="AdditionalDetails">CA: <USERTrust ECC Certification Authority> sha1: C01B8
    </EventData>
    </Event>
```

While the Microsoft documentation (#1 below) states that this can have a source name of "Microsoft-Windows-Audit-CVE" or "Audit-CVE", I have only seen this show up in Splunk as the former. Still, I wrote a rule that takes both into account.

Something else that came as a shock to me, and probably will to most other people, is that this isn't the first time Microsoft has written Windows event logs when they detect possible exploitation (ctrl+f for CVE in #2 below). Previously they used "Microsoft-Windows-Kernel-General" Event ID 1. I intend to add this to the Splunk search below that I created to watch for CVE events, but haven't had time yet to test the syntax. When I get it right, I'll update this post, so check back.

1) https://docs.microsoft.com/en-us/windows/win32/api/securitybaseapi/nf-securitybaseapi-cveeventwrite

2) https://medium.com/@synapseproject/synapse-example-extending-as-a-dataaccesslayer-api-and-integrating-with-reporting-tools-72e2b4099e5

```
index=wineventlog (SourceName="Microsoft-Windows-Audit-CVE" OR SourceName="Audit-CVE")
| rex field=Message "(?m)(?<Alert_Info>.*)"
| table _time host EventCode SourceName Alert_Info
```

Richard Davis at 13Cubed has created an excellent video covering this topic, and his video is where I learned of the previous Microsoft-Windows-Kernel-General usage. Once his video is released to the public, I'll update this post with a link to it as well. (edit: The video is now up here https://www.youtube.com/watch?v=ebmW42YYveI)

Here's a sample event if you want to play with it: https://drive.google.com/open?id=1XNFlUg5hryWWJR1uovd9WSKVzZozxmiO

AppCompatCache Part 3

In my previous post, I went though the structure of the AppCompatCache and then parsed out the actual values found. I expect this to be the last part...

Building a Custom AppCompatCacheParser.exe

Aug 27, 2024 · 11 min read

I'm still digging into the values found in my previous post (AppCompatCache Deep Dive) and as part of that, wanted to see the actual values being…

Aug 26, 2024 · 5 min read