CrowdStrike Detects Dell Driver Vulnerability CVE-2021-21551

crowdstrike.com/blog/crowdstrike-falcon-detects-dell-driver-vulnerability-cve-2021-21551/

Satoshi Tanda May 17, 2021

Vulnerabilities in the kernel mode component have serious implications on endpoint security. Operating systems and independent software vendors have been improving the security of code for years, but what happens if an endpoint is still using a kernel mode driver designed and implemented 10 years ago?

CrowdStrike reached out to Dell reporting a driver vulnerability (CVE-2021-21551) affecting the dbutil_2_3.sys kernel mode driver found in Dell's system update software used to update the BIOS. After establishing communication and receiving confirmation on the vulnerability, Dell publicly disclosed the issue on May 4, 2021, in a coordinated effort with other security researchers who reported the same issue to minimize disruptions for potentially impacted endpoints.

What makes this vulnerability stand out in dbutil_2_3.sys is that drivers are legitimately signed and can remain unpatched "in the wild" for years, significantly increasing the attack surface for adversaries.

With a CVSS base score of 8.8, its potential weaponization could impact Dell enterprise systems around the world for years. While Dell has released a security bulletin acknowledging the 10-year driver issue, **CrowdStrike Falcon® customers are protected against an attempt to exploit it.**

User Land Is Good, Kernel Mode Is King

Adversaries are constantly updating their tactics and techniques to maximize their efficiency in compromising targets while flying below the defenders' radar. The DSA-2021-088 (CVE-2021-21551) vulnerability could potentially be one such tool that once added to the adversary's toolset would allow for kernel-mode privilege escalation.

Vulnerabilities in kernel drivers can be the holy grail of adversarial tactics as they enable privilege escalation to the point where adversaries can make system changes ranging from deactivating security measures to stealing user credentials and pivoting laterally across the infrastructure.

The Dell Driver Vulnerability

DSA-2021-088 pertains to the vulnerability in Dell's dbutil_2_3.sys kernel mode driver. This driver is used by Dell's system update software to update BIOS, for example, and is embedded into, extracted from and loaded by the BIOS update executables, such as LatitudeXXXX.exe.

The issue with this driver is that it exposes multiple IOCTLs that let non-administrators perform operations that would typically require administrator privileges. As such, it allows local privilege escalation (LPE).

Some examples include but are not limited to:

- 0x9B0C1EC8 and 0x9B0C1EC4 allow arbitrary kernel memory write and read
- 0x9B0C1F44 and 0x9B0C1F40 allow arbitrary physical memory write and read
- 0x9B0C1F80, 0x9B0C1F84, 0x9B0C1F88, 0x9B0C1F8C and a few others allow access to arbitrary IO ports

All of these are LPEs for non-administrators. While there is no publicly available exploit of which we are aware as of this writing, some of these vulnerabilities are exploitable in practice. Below is an example exploitation of 0x9B0C1EC4 reading contents of kernel memory address from a non-administrator user.

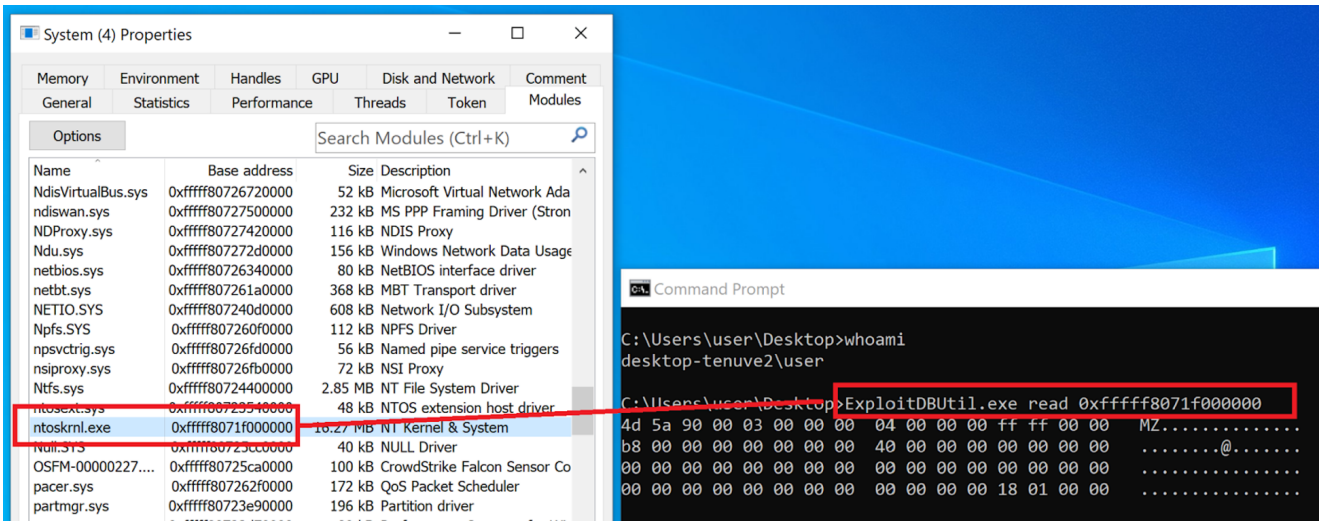

Figure 1. Reading kernel memory from non-administrator by exploiting DBUtil_2_3 (Click to enlarge)

Adding to the complexity of the issue, this driver can be automatically loaded if the endpoint has already installed Dell's system update programs and has been configured to check updates automatically. This means that an attacker would not need to drop the dbutil_2_3.sys file, elevate itself to the administrator and load the driver. All it would take is to execute a program that issues IOCTL as non-administrator, which is substantially harder to detect compared with the former scenario.

CrowdStrike's Protection

The CrowdStrike Falcon platform provides visibility into these issues and has protected endpoints from exploitation of vulnerable drivers through Additional User-Mode Data (AUMD). For more information on this, read Detecting and Preventing Kernel Attacks, which provides details on CrowdStrike coverage and additional examples.

Specifically for DSA-2021-088 (CVE-2021-21551), we provide — for endpoints with Falcon 6.18 and above — visibility against some of the above IOCTLs that are most likely to be abused in the real world. If one of those IOCTLs is exploited, it would show up in the Falcon Host UI as a high-severity detection as shown below, even if an attacker avoided the driver installation steps outlined above.

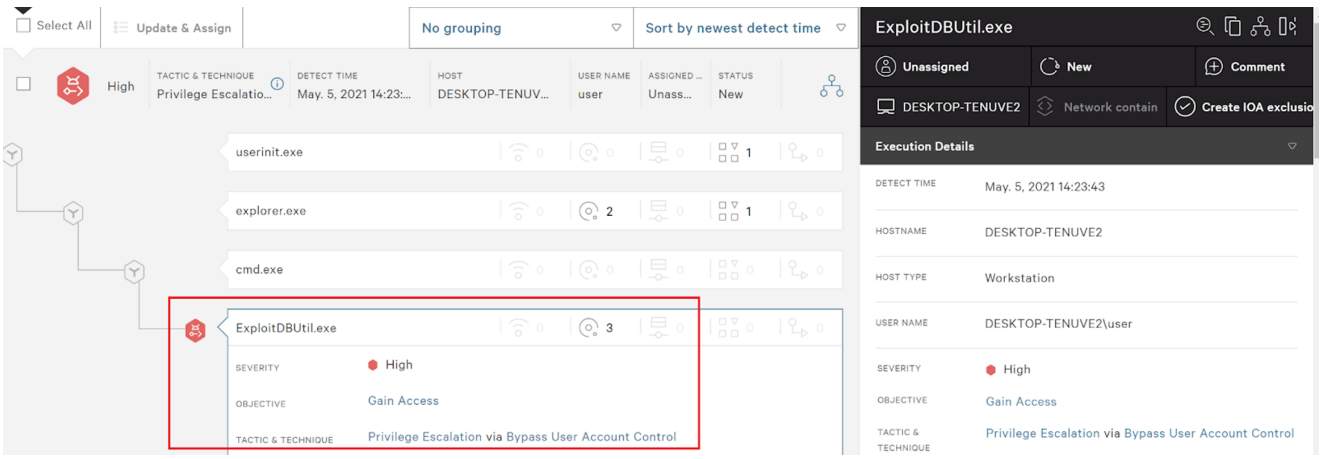

Figure 2. Detecting exploitation of IOCTL (Click to enlarge)

In addition to the protections against IOCTLs, Falcon provides users with access to Event Search, which can identify with this query how widely the vulnerable driver is loaded within the organization.

```
event_simpleName=DriverLoad SHA256HashData IN
(0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5,
87e38e7aeaaaa96efe1a74f59fca8371de93544b7af22862eb0e574cec49c7c3) | dedup aid
```

Falcon users can also query processes that initiated the loading of the driver and/or issued some of the vulnerable IOCTLs that might warrant deeper investigation, through DriverLoaded and UmppcDetectInfo events as follows:

```
event_simpleName=ProcessRollup2
    [ search event_simpleName=DriverLoad SHA256HashData IN
(0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5,
87e38e7aeaaaa96efe1a74f59fca8371de93544b7af22862eb0e574cec49c7c3)
    | where isnotnull(RpcClientProcessId_decimal)
    | rename RpcClientProcessId_decimal as TargetProcessId
    | fields TargetProcessId, aid
    ]

event_simpleName=ProcessRollup2
    [ search event_simpleName=UmppcDetectInfo DeviceName="\\Device\\DBUtil_2_3"
    | rename ContextProcessId as TargetProcessId
    | fields TargetProcessId, aid
    ]
```

CrowdStrike will monitor the active exploitation of the driver and enhance detection as we observe more cases in the wild. In the meantime, we strongly recommend making an inventory of the hosts that load the driver and remediate the issue according to the guide provided by Dell.

We would like to thank Dell for addressing the issue, as well as all community members who helped Dell to make the fix happen.

References:

- DSA-2021-088: Dell Client Platform Security Update for an Insufficient Access Control Vulnerability in the Dell dbutil Driver
- Additional Information Regarding DSA-2021-088: Dell Client Platform Security Update for an Insufficient Access Control Vulnerability in the Dell dbutil Driver

Additional Resources

- *Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Learn more about CrowdStrike endpoint detection and response by visiting the Falcon Insight™ webpage.*

- *See how you can continuously monitor and assess the vulnerabilities in your environment with Falcon Spotlight.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*