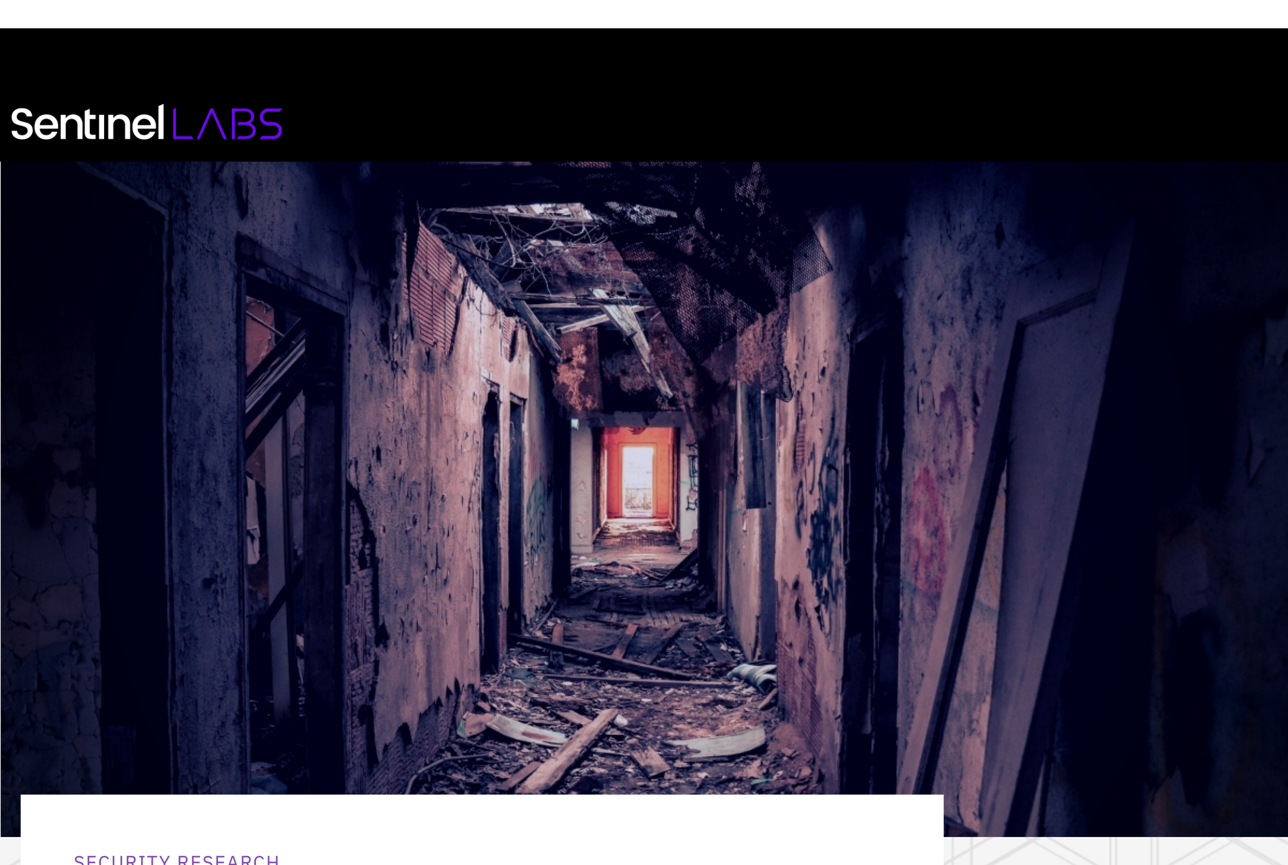
Sentinel LABS



SECURITY RESEARCH

CVE-2021-24092: 12 Years in Hiding – A Privilege Escalation Vulnerability in Windows Defender

KASIF DEKEL / FEBRUARY 10, 2021

Executive Summary

In this post, we disclose a severe vulnerability in Windows Defender that allows attackers to escalate privileges from a non-administrator user. Windows Defender is deeply integrated into the Windows operating system and is installed by default on every Windows machine (more than 1 billion devices).

Privileged services on Windows or in Windows components may contain bugs that enable malicious escalation of privileges. Attackers often use such vulnerabilities to carry out sophisticated attacks. Security products ensure device security and are supposed to prevent such attacks from happening, but what if the security product itself introduces a vulnerability? Who's protecting the protectors?

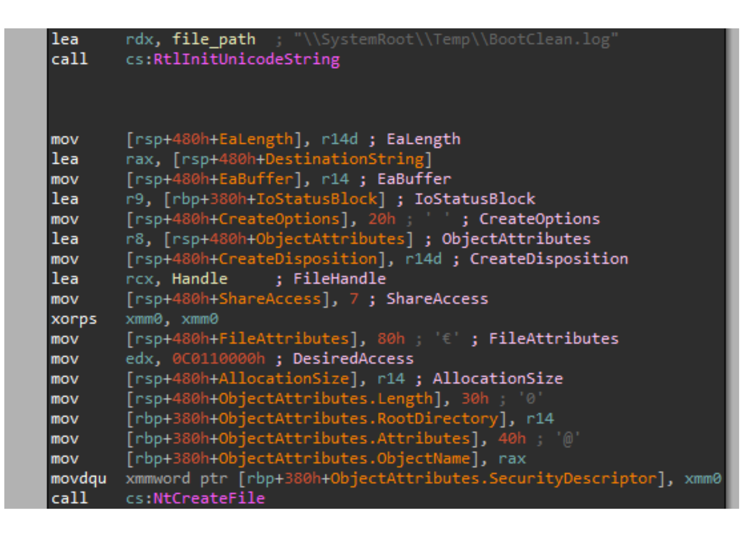
Microsoft patched the vulnerability in Windows Defender and released a fix on February 9th. Prior to the fix, the vulnerability had remained undiscovered for 12 years, probably due to the nature of how this specific mechanism is activated.

SentinelOne isn't aware of any indication that this flaw has been exploited in the wild; nevertheless, all SentinelOne customers are protected from this vulnerability.

I Was Never Here...

The driver `BTR.sys` (the driver's internal name) is part of the remediation process within Windows Defender. It is responsible for deleting file system and registry resources created by malicious software from kernel mode.

When loaded, the driver first creates a handle to a file that contains the log of its operations when activated. The problem resides in the way the driver creates the handle to this particular file, as you can see below:



```
lea     rdx, file_path  ; "\\SystemRoot\\Temp\\BootClean.log"
call    cs:RtlInitUnicodeString


mov     [rsp+480h+EaLength], r14d ; EaLength
lea     rax, [rsp+480h+DestinationString]
mov     [rsp+480h+EaBuffer], r14 ; EaBuffer
lea     r9, [rbp+380h+IoStatusBlock] ; IoStatusBlock
mov     [rsp+480h+CreateOptions], 20h ; ' ' ; CreateOptions
lea     r8, [rsp+480h+ObjectAttributes] ; ObjectAttributes
mov     [rsp+480h+CreateDisposition], r14d ; CreateDisposition
lea     rcx, Handle     ; FileHandle
mov     [rsp+480h+ShareAccess], 7 ; ShareAccess
xorps   xmm0, xmm0
mov     [rsp+480h+FileAttributes], 80h ; '€' ; FileAttributes
mov     edx, 0C0110000h ; DesiredAccess
mov     [rsp+480h+AllocationSize], r14 ; AllocationSize
mov     [rsp+480h+ObjectAttributes.Length], 30h ; '0'
mov     [rbp+380h+ObjectAttributes.RootDirectory], r14
mov     [rbp+380h+ObjectAttributes.Attributes], 40h ; '@'
mov     [rbp+380h+ObjectAttributes.ObjectName], rax
movdqu  xmmword ptr [rbp+380h+ObjectAttributes.SecurityDescriptor], xmm0
call    cs:NtCreateFile
```

The register `r14d` was previously xored with itself, which means it contains zero, so the `CreateDisposition` parameter gets the constant: `FILE_SUPERSEDE`.

`FILE_SUPERSEDE` is considered as a transaction that first deletes the original file and then creates a new file. You can notice that there is no verification whatsoever whether or not this file is a link. Thus, creating a link at `C:WindowsTempBootClean.log` would allow attackers to overwrite arbitrary files. The link is supposed to point to the file we want to overwrite. For example:

1. Create a hard link that points to notepad.exe.
2. Simulate the load of BTR for demonstration purposes, normally loaded by Windows Defender during certain remediation phase.
3. Notepad.exe is overwritten, not valid PE anymore.

We ran the following query on VirusTotal:

Surprisingly, we found versions of this driver containing the bug and signed by Microsoft *as far back as 2009*. For instance:

SHA 256
0463f8b5bd31cd1bcfe27fe00ee3cb09ef76a9a78ce0c064b6f69f7febc630f9
SHA 1 88e1668ea5a9e6e476c52a9dc629934b281e38ac

SHA 256
55d998973c182c395b5407a42b63dbb528c65d829a7af6cd08797b0ede631eef
SHA 1 019bd0060d4b4ad8c417d9e28e1fda361e85fb55

SHA 256
174122a837338648a1d88263e118781d912ae566d7f7711f08792a54028d5021
SHA 1 d45705e4566dbe9eaa7155a7296e637bedec7c70

SHA 256
c447a47c5246453c5655e6d1716f0954662fc185f28645681509d1366915cd4b
SHA 1 f0be713fcb0c766f62746273aedafbca909387b3

SHA 256
8df74468e26f7756b2ff5e75e1d83345226882a8ae2da08e251963c819ca3c5c
SHA 1 9a3d727c131308f59bc4e804fe1b79d907684b61

The bug may have existed prior to 2009, but VirusTotal only allows you to search for files uploaded within a limited time period.

We assume that this vulnerability remained undiscovered until now because the driver is normally not present on the hard drive but rather dropped and activated when needed (with a random name) and then purged away.

Mitigation

Machines that run an updated version of Windows Defender are protected against CVE-2021-24092. Recent versions of Windows 10, when updated, are protected against EoP exploits using native hard links.

Microsoft Advisory: CVE-2021-24092

Conclusion

Of course, while it seems like the vulnerability hasn't been exploited, bad actors will probably figure out how to leverage it on unpatched systems. Additionally, since the vulnerability is present in all Windows Defender versions starting from around 2009, it's likely that numerous users will fail to apply the patch, leaving them exposed to future attacks.

SentinelOne's customers are protected from this vulnerability as this driver won't be loaded when the SentinelOne agent is installed.

Using such a vulnerability to run code is often more tricky but not impossible; certain primitives are needed to be utilized, but this can still be used for various malicious activities such as disabling security products.

Disclosure Timeline

Nov 16, 2020 – Initial report sent to MSRC.
Nov 16, 2020 – Initial response from MSRC stating they're looking into it.
Nov 30, 2020 – MSRC acknowledged that they reproduced the bug and started working on it.
Feb 09, 2021 – MSRC Released a patch.

CVE | DRIVERS | PRIVILEGE ESCALATION | VULNERABILITY | WINDOWS DEFENDER

KASIF DEKEL

Kasif Dekel is a passionate Senior Security Researcher at SentinelOne focusing on low level research, studying operating systems, malware, and system vulnerabilities for the benefit of the company's security products.