CVE-2022-32230: Windows SMB Denial-of-Service Vulnerability (FIXED)

Jun 14, 2022 | 3 min read |
Spencer McIntyre (/blog/author/spencer-mcintyre/)

Last updated at Tue, 14 Jun 2022 17:10:06 GMT

A remote and unauthenticated attacker can trigger a denial-of-service condition on Microsoft Windows Domain Controllers by leveraging a flaw that leads to a null pointer deference within the Windows kernel. We believe this vulnerability would be scored as CVSSv3 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?

Topics

- Metasploit (797) (/blog/tag/metasploit/)
- Vulnerability Management (415) (/blog/tag/vulnerability-management/)
- Detection and Response (386) (/blog/tag/detection-and-response/)
- Research (277) (/blog/tag/research/)
- Application Security (156) (/blog/tag/application-security/)
- Cloud Security (103) (/blog/tag/cloud-security/)

vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1) or 7.5. This vulnerability was silently patched by Microsoft in April of 2022 in the same batch of changes that addressed the unrelated CVE-2022-24500 vulnerability.

Credit

This issue was fixed by Microsoft without disclosure in April 2022, but because it was originally classed as a mere stability bug fix, it did not go through the usual security issue process. In May, Spencer McIntyre of Rapid7 discovered this issue while researching the fix for CVE-2022-24500 and determined the security implications of CVE-2022-32230. It is being disclosed in accordance with Rapid7's vulnerability disclosure policy (https://www.rapid7.com/security/disclosure/).

Exploitation

CVE-2022-32230 is caused by a missing check in

srv2!Smb2ValidateFileObjectOnTarch

Popular Tags

Search Ta

Metasploit (/blog/tag/metasploit/)

Logentries (/blog/tag/logentries/)

IT Ops (/blog/tag/it-ops/)

Vulnerability Management (/blog/tag/vulnerability-management/)

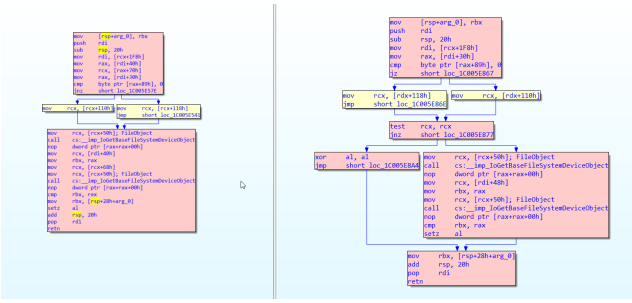
Detection and Response (/blog/tag/detection-and-response/)

Metasploit Weekly Wrapup (/blog/tag/metasploit-weekly-wrapup/)

Research (/blog/tag/research/)

Automation and Orchestration (/blog/tag/automation-and-orchestration/)

to verify that a pointer is not null before reading a `PDEVICE_OBJECT` from it and passing it to `IoGetBaseFileSystemDeviceObject`. The following patch diff shows the function in question for Windows 10 21H2 (unpatched version 10.0.19041.1566 on the left).



This function is called from the dispatch routine for an SMB2 `QUERY_INFO` request of the `FILE_INFO / FILE_NORMALIZED_NAME_INFORMATION` class. Per the docs in MS-SMB2 section 3.3.5.20.1 Handling SMB2_0_INFO_FILE (https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/d64e0451-64a2-425a-848e-52a7dddab7b9), `FILE_NORMALIZED_NAME_INFORMATION` is only available when the dialect is 3.1.1.

For FileNormalizedNameInformation

Nexpose (/blog/tag/nexpose/)

Incident Detection (/blog/tag/incident-detection/)

InsightIDR (/blog/tag/insightidr/)

Exploits (/blog/tag/exploits/)

Incident Response (/blog/tag/incident-response/)

Komand (/blog/tag/komand/)

Penetration Testing (/blog/tag/penetration-testing/)

Related Posts

READ MORE (/BLOG/POST/2022/11/2022-41622-AND-CVE-2022-

information class requests, if not supported by the server implementation<392>, or if Connection.Dialect is "2.0.2", "2.1" or "3.0.2", the server MUST fail the request with STATUS_NOT_SUPPORTED.

To trigger this code path, a user would open any named pipe from the IPC$ share and make a `QUERY_INFO` request for the `FILE_NORMALIZED_NAME_INFORMATION` class. This typically requires user permissions or a non-default configuration enabling guest access. This is not the case, however, for the noteworthy exception of domain controllers where there are multiple named pipes that can be opened anonymously, such as `netlogon`. An alternative named pipe that can be used but does typically require permissions is the `srvsvc` pipe.

Under normal circumstances, the `FILE_NORMALIZED_NAME_INFORMATION` class would be used to query the normalized name information of a file

CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and Exposures

41800-FIXED-F5-BIG-IP-AND-ICONTROL-REST-VULNERABILITIES-AND-EXPOSURES/)

READ MORE

CVE-2022-3786 and CVE-2022-3602: Two High-Severity Buffer Overflow Vulnerabilities in OpenSSL Fixed

(/BLOG/POST/2022/11/2022-3786-AND-CVE-2022-3602-TWO-HIGH-SEVERITY-BUFFER-OVERFLOWS-IN-OPENSSL-FIXED/)

READ MORE

that exists on disk. This differs from the exploitation scenario which queries a named pipe.

A system that has applied the patch for this vulnerability will respond to the request with the error `STATUS_NOT_SUPPORTED`.

Proof of concept

A proof-of-concept Metasploit module is available on GitHub (https://github.com/zeroSteiner/metasploit-framework/blob/feat/mod/cve-2022-32230/modules/auxiliary/dos/smb/smb_filenormalizednameinformation.rb). It requires Metasploit version 6.2 or later.

Impact

The most likely impact of an exploit leveraging this vulnerability is a denial-of-service condition. Given the current state of the art of exploitation, it is assumed that a null pointer dereference in the Windows kernel is not remotely exploitable for the purpose of arbitrary code execution without corrupting it with [illegible]

CVE-2021-39144: VMware Cloud Foundation Unauthenticated Remote Code Execution (/blog/post/2022/10/2021-39144-vmware-cloud-foundation-unauthenticated-remote-code-execution/)

READ MORE

New Research: We're Still Terrible at Passwords; Making it Easy for Attackers (/blog/post/2022/10/research-were-still-terrible-at-passwords-making-it-easy-for-attackers/)

another, unrelated vulnerability.

In the default configuration, Windows will automatically restart after a BSOD.

Remediation

It is recommended that system administrators apply the official patches provided by Microsoft in their April 2022 update. If that is not possible, restricting access and disabling SMB version 3 can help remediate this flaw.

Disclosure timeline

April 12th, 2022 – Microsoft patches CVE-2022-32230

April 29th, 2022 – Rapid7 finds and confirms the vulnerability while investigating CVE-2022-24500

May 4th, 2022 – Rapid7 contacts MSRC to clarify confusion regarding CVE-2022-32230

May 18th, 2022 – Microsoft responds to Rapid7, confirming that the vulnerability now identified as CVE-2022-32230 is different from the

disclosed vulnerability CVE-2022-24500 with which it was patched

June 1, 2022 — Rapid7 reserves CVE-2022-32230 after discussing with Microsoft

June 14th, 2022 – Rapid7 releases details in this disclosure, and Microsoft publishes its advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-32230)

Additional reading:

- *The Hidden Harm of Silent Patches (https://www.rapid7.com/blog/post/2022/06/06/the-hidden-harm-of-silent-patches/)*
- *CVE-2022-22977: VMware Guest Authentication Service LPE (FIXED) (https://www.rapid7.com/blog/post/2022/05/24/cve-2022-22977-vmware-guest-authentication-service-lpe-fixed/)*
- *A Year on from the Ransomware Task Force Report (https://www.rapid7.com/blog/post/2022/05/24/a-*

year-on-from-the-ransomware-task-force-report/)

- *CVE-2022-30525 (FIXED): Zyxel Firewall Unauthenticated Remote Command Injection (https://www.rapid7.com/blog/post/2022/05/12/cve-2022-30525-fixed-zyxel-firewall-unauthenticated-remote-command-injection/)*
  (https://www.rapid7.com/blog/post/2022/05/24/a-year-on-from-the-ransomware-task-force-report/)

  (https://www.rapid7.com/blog/post/2022/05/24/a-year-on-from-the-ransomware-task-force-report/)

POST TAGS

Vulnerability Disclosure (/blog/tag/vulnerability-disclosure/)

Vulnerability Risk Management (/blog/tag/vulnerability-risk-management/)

Research (/blog/tag/research/)

AUTHOR

Spencer McIntyre (/blog/author/spencer-mcintyre/)

VIEW SPENCER'S POSTS

SHARING IS CARING

Related Posts

VULNERAB…

CVE-2022-41622 and CVE-2022-41800

EMERGEN…

CVE-2022-3786 and CVE-2022-3602: Two High-

VULNERAB…

CVE-2021-39144: VMware Cloud Foundation

RESEARCH

New Research: We're Still Terrible at

VIEW ALL POSTS

Search all the things

BACK TO TOP

(/)

CUSTOMER SUPPORT

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

SALES SUPPORT

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

Need to report an Escalation or a Breach?

CLICK HERE (/services/incident-response-customer-escalation/)

SOLUTIONS

All Solutions (https://www.rapid7.com/solutions)

Industry Solutions (https://www.rapid7.com/solutions/industry)

Compliance Solutions (https://www.rapid7.com/solutions/compliance/)

SUPPORT & RESOURCES

Product Support (https://www.rapid7.com/for-customers)

Resource Library (https://www.rapid7.com/resources)

Customer Stories (https://www.rapid7.com/about/customers)

Events & Webcasts (https://www.rapid7.com/about/events-webcasts)

Training & Certification (https://www.rapid7.com/services/training-certification)

IT & Security Fundamentals (https://www.rapid7.com/fundamentals)

Vulnerability & Exploit Database (https://www.rapid7.com/db)

ABOUT US

Company (https://www.rapid7.com/about/company)

Diversity, Equity, and Inclusion (https://www.rapid7.com/about/diversity-equity-and-inclusion/)

Leadership (https://www.rapid7.com/about/leadership)

News & Press Releases (https://www.rapid7.com/about/news)

Public Policy (https://www.rapid7.com/about/public-policy)

Open Source (https://www.rapid7.com/open-source/)

Investors (https://investors.rapid7.com/)

CONNECT WITH US

Contact (https://www.rapid7.com/contact)

Blog (https://blog.rapid7.com/)

Support Login (https://support.rapid7.com/)

Careers (https://www.rapid7.com/careers)

(https://www.rapid7.com/rapid7/)

 (https://www.rapid7.com/about/rapid7-cybersecurity-partner-boston-bruins/)

 Legal Terms (/legal/) | Privacy Policy (/privacy-policy/) | Export Notice (/export-notice/) | Trust (/trust/)