CVE-2022-24527: Microsoft Connected Cache Local Privilege Escalation (Fixed)

Apr 12, 2022 | 4 min read |

Jake Baines

Last updated at Tue, 12 Apr 2022 20:03:05 GMT

On April 12, 2022, Microsoft published CVE-2022-24527 , a local privilege escalation

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

privileged user to execute arbitrary Powershell as `SYSTEM` due to improper file permission assignment (CWE-732).

Product description

Connected Cache is a feature used by Microsoft Endpoint Manager "Distribution Points " to support "Delivery Optimization."

Credit

This issue was discovered and reported by security researcher Jake Baines as part of Rapid7's vulnerability disclosure program.

Exploitation

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research

Logentries

Detection and Response

Related Posts

Ransomware Groups Demystified: CyberVolk Ransomware READ MORE

CVE-2024-45195: Apache OFBiz Unauthenticated Remote Code Execution (Fixed) READ MORE

Preparing for Unknown Risks:

Contact Us

`C:\Doinc\`. Below, you can see that there are some Powershell scripts within that directory:

```
C:\>dir /s /b C:\Doinc\
C:\Doinc\Product
C:\Doinc\Product\Install
C:\Doinc\Product\Install\Logs
C:\Doinc\Product\Install\Tasks
C:\Doinc\Product\Install\Tasks
C:\Doinc\Product\Install\Tasks
C:\Doinc\Product\Install\Tasks
```

Low-privileged users only have `read` and `execute` permissions on the Powershell scripts.

```
C:\Doinc\Product\Install\Task
CacheNodeKeepAlive.ps1 NT AUTH
                       NT AUTH
                       BUILTIN
                       BUILTIN

Maintenance.ps1 NT AUTHORITY\S
                NT AUTHORITY\N
                BUILTIN\Admini
                BUILTIN\Users:

SetDrivesToHealthy.ps1 NT AUTH
```

```
Successfully processed 3 files
```

The Powershell scripts are executed every 60 seconds by the Task Scheduler as `NT AUTHORITY\SYSTEM`. All that is fine. The following part is where trouble begins. This is how `SetDrivesToHealthy.ps1` starts:

```
try
{
    import-module 'webAdminist

    $error.clear()
```

When `SetDrivesToHealthy.ps1` executes, it attempts to load the `webAdministration` module. Before searching the normal %PSModulePath% path, `SetDrivesToHealthy.ps1` looks for the import in `C:\Doinc\Product\Install\Tasks\WindowsPowerShell\Modules\webAdmin`

As we saw above, this directory

scripts, they do have sufficient privileges to add subdirectories and files to `C:\Doinc\Product\Install\Tasks\`:

```
C:\Doinc\Product\Install>icac
./Tasks/ NT AUTHORITY\SYSTEM:(
         NT AUTHORITY\NETWORK
         BUILTIN\Administrator
         BUILTIN\Users:(I)(OI)
         BUILTIN\Users:(I)(CI)
         BUILTIN\Users:(I)(CI)
         CREATOR OWNER:(I)(OI)
```

An attacker can create the necessary directory structure and place their own `webAdministration` so that `SetDrivesToHealthy.ps1` will import it. In the proof of concept below, the low-privileged attacker creates the directory structure and creates a PowerShell script that creates the file `C:\r7`.

Contact Us

```
 Directory of C:\

01/04/2022  05:01 PM    <DIR>
01/04/2022  05:15 PM    <DIR>
01/04/2022  03:48 PM    <DIR>
07/07/2021  04:05 AM    <DIR>
01/05/2022  09:29 AM    <DIR>
01/05/2022  09:29 AM    <DIR>
01/05/2022  09:16 AM    <DIR>
01/05/2022  09:15 AM    <DIR>
01/05/2022  09:17 AM    <DIR>
01/05/2022  09:17 AM    <DIR>
01/04/2022  05:04 PM    <DIR>
01/04/2022  03:48 PM    <DIR>
               0 File(s)
              12 Dir(s)  239,8

C:\Doinc\Product\Install\Tasks

C:\Doinc\Product\Install\Tasks

C:\Doinc\Product\Install\Tasks

C:\Doinc\Product\Install\Tasks

C:\Doinc\Product\Install\Tasks
 Volume in drive C has no labe
 Volume Serial Number is 3073-

 Directory of C:\

01/04/2022  05:01 PM    <DIR>
01/04/2022  05:15 PM    <DIR>
01/04/2022  03:48 PM    <DIR>
```

Contact Us

```
01/05/2022  09:16 AM    <DIR>
01/05/2022  09:15 AM    <DIR>
01/05/2022  09:17 AM    <DIR>
01/05/2022  09:17 AM    <DIR>
01/04/2022  05:04 PM    <DIR>
01/04/2022  03:48 PM    <DIR>
               1 File(s)
              12 Dir(s)  239,8

C:\Doinc\Product\Install\Tasks
C:\lol.txt NT AUTHORITY\SYSTEM
           BUILTIN\Administrat
           BUILTIN\Users:(I)(R

Successfully processed 1 files

C:\Doinc\Product\Install\Tasks
```

As you can see, the `C:\r7.txt` file is created, demonstrating the privilege escalation.

Remediation

Follow Microsoft guidance on updating the Distribution Point software. If that is not possible, disabling the caching feature

Disclosure timeline

January 5, 2022: Issue disclosed to the vendor

January 5, 2022: Vendor acknowledgement

January 6, 2022: Vendor assigns a case identifier

January 10-11, 2022: Vendor and researcher discuss clarifying details

January 19, 2022: Vendor confirms the vulnerability

February-March 2022: Vendor and researcher coordinate on disclosure date and CVE assignment

April 12, 2022: Public disclosure (this document)

Additional reading:

Contact Us

- *Analyzing the Attack Landscape: Rapid7's 2021 Vulnerability Intelligence Report*
- *Cloud Pentesting, Pt. 1: Breaking Down the Basics*
- *CVE-2021-4191: GitLab GraphQL API User Enumeration (FIXED)*

POST TAGS

Risk Management

SHARING IS CARING

AUTHOR

Jake Baines

VIEW JAKE'S POSTS

Related Posts

LABS

Ransomware Groups Demystified: CyberVolk Ransomware

VULNERABILITY DISCLOSURE

CVE-2024-45195: Apache OFBiz Unauthenticated Remote Code Execution (Fixed)

Contact Us

RISK MANAGEMENT

Preparing for Unknown Risks: How to Better Prepare for Risks You Can't See Yet

READ FULL POST

REPORTS

New Research: The Proliferation of Cellular in IoT

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

Contact Us

RAPID7

Select

START TRIAL

Our Customers

Events & Webcasts

Training & Certification

Cybersecurity Fundamentals

Vulnerability & Exploit Database

Leadership

News & Press Releases

Public Policy

Open Source

Investors

CONNECT WITH US

Contact

Blog

Support Login

Careers

Legal Terms Privacy Policy Export Notice Trust
Do Not Sell or Share My Personal Information Cookie Preferences

Contact Us