Tiger-Team-1337

Tuesday, October 13, 2020

Solstice-Pod - Critical Unauthenticated Remote DoS Vulnerability

Date: 2020-09-30

Author: Kevin2600

CVE: CVE-2020-27523

Version: Gen2i-Pod (5.0.2)

Vendor:

https://documentation.mersive.com/content/home.htm

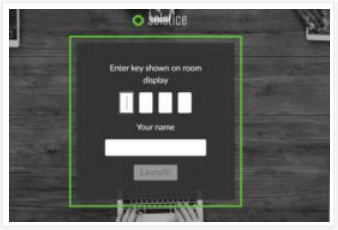
https://documentation.mersive.com/content/topics/general-gen2i-pod-specs.htm

Attack-Vector:

When users try to connect to the Solstice-Pod, the correct screen key is needed in order to authenticate the user. Even appears to be only digit number can be accepted for the screen key. But we can still inject format-string specifiers like "%x", And this will cause Solstice-Pod to reboot, which lead to a DoS attack.

Reproduce-Steps:

1: Connect to Solstice-Pod with browser for screen sharing. It asks to input the screen key.



2: Using BurpSuite to intercept the access URL path and replace the screen key value with format-string specifiers like "%x".

```
https://IP:6443/webrtc?screen_key=%x&display_name=kevin2600&browser_name=Firefox&operation_system=Linux
```

3: The Solstices-Pod will be reboot immediately, Screen went blank and restart takes about 20-30 seconds.

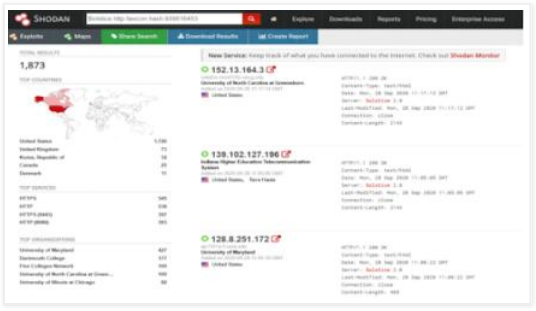
Impact-Level:

Blog Archive

May 2022 (1)
January 2022 (1)
January 2021 (1)
October 2020 (2)

Report Abuse

According to Search engine ZoomEye, Shodan, and FoFa. Currently, more than 17,117 Solstice-pods exposed to the public on the Internet. And because this is an Unauthenticated Remote DoS Vulnerability, the impact is critical.



Vendor response:

1) The Vendor Mersive has been contacted on SEPT 28th

2) The full detail and video demo have been sent based on Mersive requested on OCT 8th

3) Mersive replied on OCT 15th, their Dev team is currently investigating the bug. They are able to confirm and generate a fix for this. It will be in the 5.2 release.

at October 13, 2020

No comments:

Post a Comment

To leave a comment, click the button below to sign in with

Newer Post Home

Subscribe to: Post Comments (Atom)