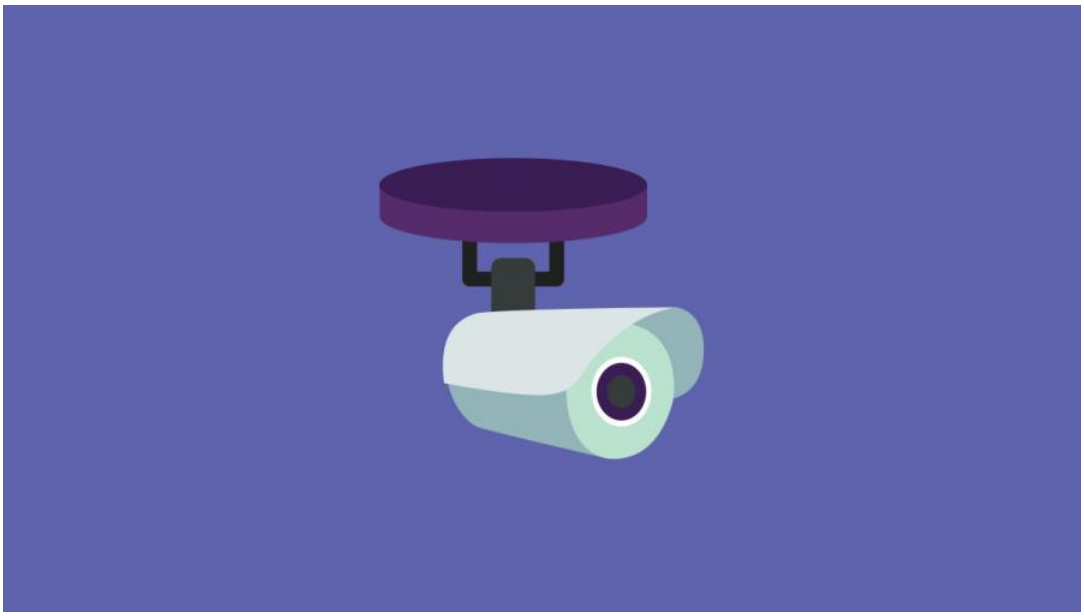
The Daily Swig
Cybersecurity news and views

Researcher discloses alleged zero-day vulnerabilities in NUUO NVRmini2 recording device

Charlie Osborne 14 January 2022 at 16:30 UTC
Updated: 17 January 2022 at 16:07 UTC

Zero-day | RCE | Vulnerabilities

Exploit code has also been released for flaws that supposedly date back to 2016



A critical 'zero-day' vulnerability in network video recording equipment made by NUUO has been made public, as a researcher claims unpatched issues could lead to remote code execution (RCE).

Discovered by Agile Information Security founder Pedro Ribeiro, the issues have allegedly been present in the NUUO NVRmini2 device since 2016.

NVRmini2 is a network video recorder (NVR) from Taiwanese vendor NUU that is able to record and store security footage in a digital format.

Read more of the latest zero-day vulnerability news

Ribeiro claims he disclosed command injection and stack overflow vulnerabilities in NVRmini2 six years ago. At the time, Ribeiro said that the product had "terrible security" – and if his claims are true, then nothing has changed for the better.

"Both vulnerabilities disclosed were found during my 2016 audit," Ribeiro told *The Daily Swig*. "However, at the time, I found so many other vulnerabilities that I actually forgot to report these – until in 2019 when I rediscovered my notes and reported it to them."

Unpatched issues

As documented on GitHub, there are apparently two unpatched vulnerabilities. The first, yet to be assigned a CVE but considered critical, is a missing authentication method on a critical function in NVRmini2 firmware.

The `handle_import_user.php` function for every firmware version up to and including the latest build lacks adequate protections to stop unauthenticated users from accessing the script, claims Ribeiro.

The second alleged vulnerability is the use of a legacy version of BusyBox, a Unix utilities package. This version is impacted by a range of bugs including CVE-2011-5325, a path traversal flaw that allows remote attackers to point to files outside of the current, working directory.

Latest Posts

ConnectWise closes XSS vector f
remote hijack scams
Researchers also applaud abandonment
customization feature abused by scamme

AWS AppSync bug left cloud
resources vulnerable
Attackers could gain full control of a cloud
hosted database

Mastodon vulnerable to multiple
system config problems
The whole toot

By abusing the HTTP POST mechanism and crafting malicious tar archives, it is possible to chain the vulnerabilities in order to drop a webshell and execute commands as root, says Ribeiro.

YOU MAY ALSO LIKE Bug Alert launched to provide early warning system for super-critical zero-day vulnerabilities

In addition to the disclosure, the researcher has released a Metasploit module which packages up the vulnerability chain described in the advisory.

The Proof-of-Concept (PoC) code is said to work on most firmware versions with the exception of those older than version 2.0.0 – although alternative techniques can be used on legacy software versions.

At the time of writing, the vulnerabilities remain unpatched on the latest firmware version, v.03.11.0000.0016, despite the researcher claiming he made multiple attempts to disclose them. No official fix is available.

Mitigating risks

The researcher recommends that NVRmini2 device owners keep their products away from untrusted networks as a way to mitigate the risk of exploitation.

Aside from that, using Ribeiro's own exploit and deleting the `handle_import.user.php` function may fix the issue, but this is not guaranteed.

"During the disclosure process, even after multiple attempts, they didn't really seem to understand the vulnerability," Ribeiro commented.

"We explained it to them several times, and they seemed completely clueless. They were quite nice and pleasant to deal with it in terms of manners and how they treated us, but technically clueless."

The Daily Swig has reached out to NUUO for comment but has not heard back at the time of publication. We will update this article as and when we hear back.

RECOMMENDED GitLab shifts left to patch high-impact vulnerabilities

Zero-day | RCE | Vulnerabilities | Hardware | Asia | Network Security | Secure Development | Surveillance | Industry News | Research | Path Traversal | IoT | Organizations | Hacking News | Hacking Techniques

Charlie Osborne

@SecurityCharlie

Related stories

ConnectWise closes XSS vector for remote hijack scams

25 November 2022

AWS AppSync bug left cloud resources vulnerable

25 November 2022

Mastodon vulnerable to multiple system config problems

22 November 2022

Ibexa DXP patched for GraphQL password hash leak

18 November 2022