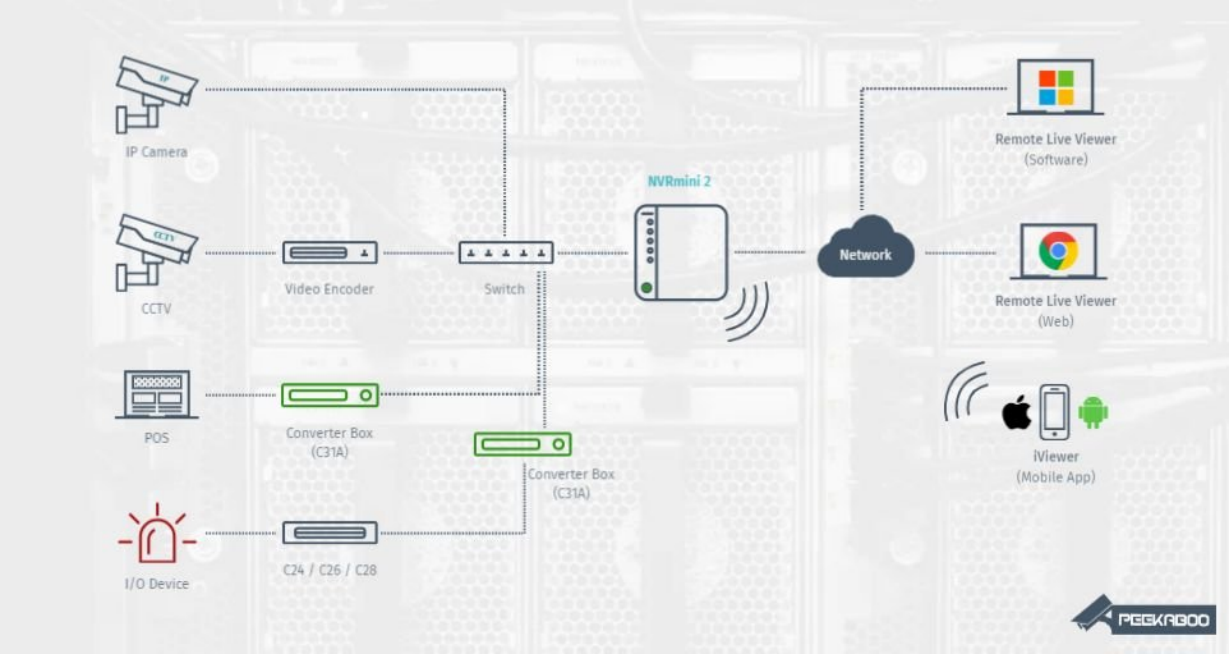
Tenable Research discloses Peekaboo vulnerability affecting video surveillance

September 19 2018, by Nancy Owano



Hackers have proven capable of staging a hijack of surveillance camera footage. Security hounds are calling the zero day vulnerability Peekaboo. In brief, certain internet-connected surveillance cameras, could be vulnerable to remote takeover. "Once exploited, Peekaboo would give cybercriminals access to the control management system (CMS), exposing the credentials for all connected video surveillance cameras,"

said Tenable Research.

Charlie Osborne for *ZDNet* said on Monday that the bug was disclosed by Tenable Research, a cybersecurity group.

Actually, you can check out the Tenable site for a complete description of what their sleuths found and why it matters. Tenable Research in a news release said that it had disclosed the vulnerability, which affects firmware versions older than 3.9.0, to NUUO.

The bug was assigned as CVE-2018-1149.

Tenable said the vulnerability named Peekaboo was about "permitting remote code execution in IoT network video recorders for video surveillance systems that would allow attackers to remotely view feeds and tamper with recordings."

The vulnerable device taking center stage is NVRMini2. It is from NUUO, which offers closed-circuit television (CCTV), surveillance and video software and hardware. NUUO's software is deployed by many video surveillance systems all over the world. A news release from Tenable noted that "NUUO software and devices are commonly used for web-based video monitoring and surveillance in industries such as retail, transportation, education, government and banking."

What is NVRMini2? Shaun Nichols in *The Register* said it is "a network-attached device that both stores video recordings and acts as a control gateway for admins and remote viewers."

Tenable's discussion said that this is how multiple camera feeds can be viewed and recorded simultaneously.

"We found an unauthenticated stack buffer overflow...permitting remote

code execution. This vulnerability has a CVSSv2 Base score of 10.0 and a Temporal Score of 8.6; it's rated as Critical severity." They said they also found a backdoor in leftover debug code.

What could happen if criminals were to achieve an exploit? Tenable said "cyber criminals could disconnect the live feeds and tamper with security footage."

The good news is that NUUO has informed Tenable that a patch is being developed and affected customers should contact NUUO for further information. (At the time of this writing on September 18, a time list on the Tenable site dated 09-17-2018—said "NUUO says there will be a release tomorrow.")

"In the meantime," said Tenable, "we advise affected end users to restrict and control network access to the vulnerable devices to authorized and legitimate users only." Also, Tenable released a plugin to assess whether organizations are vulnerable to Peekaboo.

Renaud Deraison, co-founder and CTO of Tenable, also had some observations to make about the bigger picture, in an interview with *Threatpost*. "We believe vulnerable IoT devices such as these raise serious questions about how we as an industry can manage large numbers of devices. Even in a corporate environment, if the number of connected devices grows at the forecasted rate, we are going to need to rethink our patching cadence and methodology," he said.

More information: www.tenable.com/security/research/tra-2018-25

Citation: Tenable Research discloses Peekaboo vulnerability affecting video surveillance (2018,

September 19) retrieved 28 April 2024 from https://techxplore.com/news/2018-09-tenable-discloses-peekaboo-vulnerability-affecting.html