Plug-and-play bug exposes millions of network devices

12 June 2020, by Peter Grad

Credit: Pixabay/CC0 Public Domain

A bug in a protocol used by virtually all Internet of Things devices exposes millions of users to potential attack, a researcher reported Monday. The fault centers on the Universal Plug and Play protocol, a 12-year-old implementation that simplifies connections among network devices such as computers, printers, mobile devices and Wi-Fi access points.

Billions of devices are theoretically vulnerable, the report stated, but only those with UPnP activated currently face risk of attack.

Turkish security engineer Yunus Çadirci uncovered the UPnP bug, named CallStranger, that could be exploited to gain access to any smart device such as security cameras, printers and routers that are connected to the Internet. Once access is gained, malicious code can be sent through network firewalls and other security defenses and reach internal data banks.

The bug also permits attackers to surreptitiously amass huge numbers of devices to engage in denial-of-service attacks that flood targets with traffic, block legitimate traffic, overwhelm processing resources and cause the systems to crash.

Çadirci operates a website dedicated to information about the CallStranger vulnerability. He first detected it late last year and notified the Open Connectivity Foundation, which has since updated UPnP specifications to address the issue. Vendors and Internet service providers requested notice of the vulnerability be withheld until they had time to address the issue.

"Because this is a protocol vulnerability, it may take a long time for vendors to provide patches," Çadirci said in his report. Since some manufacturers have not yet corrected the issue and many IoT devices never receive updates, consumers should contact manufacturers of any UPnP devices they use to determine if software or hardware patches are available.

Universal Plug and Play has long been known to leave users vulnerable to attacks. A 2013 research project confirmed that more than 81 million devices that presumably were protected within local networks were in fact visible to potentially malicious actors beyond those networks.

"We see data exfiltration as the biggest risk of CallStranger," Çadirci said. "Checking logs is critical if any threat actor used this in the past. Because it also can be used for distributed denial of service requests, we expect botnets will start implementing this new technique by consuming end-user devices."

Security experts advise users to disable UPnP on devices connected to the Internet if their businesses do not require such connections. Routers generally allow UPnP to be disabled by unchecking a box in the settings menu.

While the bug affects virtually all UPnP devices, Çadirci tested and confirmed vulnerabilities in a few

dozen devices including those from Microsoft, Asus, Broadcom, Cisco, D-Link, Epson, HP, Huawei, NEC, Philips and Samsung.

Çadirci explained that attackers transmit TCP packets with manipulated callback header values using UPnP's SUBSCRIBE function. This lets an invader tap into devices with continuous connections to the Internet.

More information: callstranger.com/

© 2020 Science X Network
APA citation: Plug-and-play bug exposes millions of network devices (2020, June 12) retrieved 29 September 2022 from https://techxplore.com/news/2020-06-plug-and-play-bug-exposes-millions-network.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.