CISA Warns of Security Holes in Industrial Advantech, Hitachi Kit

October 20, 2022 06:54:04 PM, 22-00024114

FROM THE MEDIA

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two new vulnerabilities (CVE-2022-3386, CVE-2022-3385) affecting industrial appliances manufactured by Advantech and Hitachi Energy to its Known Exploited Vulnerabilities Catalog. CISA also issued two alerts related to security flaws impacting Advantech's R-SeeNet that could be exploited by remote attackers to take complete control of industrial network router monitoring software or to completely delete PDF files from the system. According to CISA, CVE-2022-3386 and CVE-2022-3385 are stack-based buffer overflow issues impacting versions 2.4.17 and earlier of the R-SeeNet software and can both be exploited by "an unauthorized attacker [to] use an outsized filename to overflow the stack buffer and enable remote code execution." CISA also noted a third traversal vulnerability that affects version 2.4.19 of the R-SeeNet software that could be leveraged by attackers to exploit vulnerable PHP code and delete PDF files. Advantech is now recommending that organizations immediately update R-SeeNet software to version 2.4.21 or later. CISA also advises organizations to minimize appliances' and control systems devices' internet exposure to the public internet. CISA also says local control system network and remote devices should be isolated from business networks and located behind firewalls.

READ THE STORY: The Register

NEWS ANALYSIS RATING: ✔ MEDIA ON-TARGET

ANALYST COMMENT

Mandiant would rate CVE-2022-3386 and CVE-2022-3385 to be high risk due to the potential for remote code execution. Advantech has released fixes that reportedly address these issues. Mandiant recommends prioritizing the patching of vulnerable systems. Exploit code is not currently publicly available, and there is no evidence of exploitation in the wild. Media on-target.

Related Intelligence Report(s):

September 2022 Month in Vulnerabilities SUBSCRIPTION REQUIRED	October 12, 2022 11:41:40 AM | 22-00023297
Weekly Vulnerability Exploitation Report – Oct. 17, 2022 SUBSCRIPTION REQUIRED	October 17, 2022 07:09:28 PM | 22-00023905

About this Product

The expert analysts at FireEye Intelligence highlight and provide context to current media trends each day as they analyze and encapsulate the events in cyber security. Topics selected cover a broad array of cyber threats and are intended to aid readers in framing key publically discussed threats. FireEye does not specifically endorse any third-

party claims made in this material or related links, and the opinions expressed by third parties are theirs alone. The enclosed FireEye Intelligence comments and accuracy rankings are based on information available at the time of publication, and FireEye reserves the right to hone its analytical perspectives as the threats evolve and as further intelligence is made available.

MEDIA ON-TARGET

This ranking denotes a media trend in which the information reported is generally verifiable and can be correlated with our additional intelligence sources.

PLAUSIBLE

This ranking refers to a story possessing key information that, although plausible based off our past observations of similar events, we have not been able to validate in the short time available.

JUDGMENT WITHHELD

This ranking refers to a story which is complex enough that we cannot validate it in a short time.

MEDIA OFF-TARGET

This ranking refers to a story in which key elements are unsubstantiated or inaccurate. A story can have a key element which is inaccurate, and the rest accurate, and still receive the ranking Off Target.

The accuracy rating is applied through analysis of the data behind each trend based on FireEye closed sources of information. The reason for this rating is so that our readers can quickly be alerted to trends, which are not yet substantiated or are based on information in conflict with FireEye findings. This document is developed and provided by FireEye Intelligence for direct distribution to your organization. Re-distribution or publication outside of your organization is not permitted without the expressed written permission of FireEye.

MANDIANT ADVANTAGE

german[.]simkin@mandiant.com