Trend Micro antivirus zero-day used Mitsubishi Electric hack

Hackers exploited a Trend Micro OfficeScan zero-day to plant malicious files on Mitsubishi Electric servers.

Written by **Catalin Cimpanu,** Contributor
Jan. 24, 2020 at 12:51 p.m. PT

Chinese hackers have used a zero-day in the Trend Micro OfficeScan antivirus during their attacks on Mitsubishi Electric, ZDNet has learned from sources close to the investigation.

Trend Micro has now patched the vulnerability, but the company did not comment if the zero-day was used in other attacks beyond Mitsubishi Electric.

Mitsubishi Electric hack

News of the Mitsubishi Electric hack became public on Monday, this week. In a press release published on its website, the Japanese

ZDNET INNOVATION INDEX

rank		trend
1	new	Google now shows AI
2	new	Google Maps introduces
3	new	Microsoft integrates
4	new	Claude 3 LLM surpasses

read full trend report

/ related

Are yo devic will sc secur

Every know Micro Serve

Nvidia Micro and G redes Innov

electronics vendor and defense contractor said it was hacked last year.

The company said it detected an intrusion on its network on June 28, 2019. Following a months-long investigation, Mitsubishi said it discovered that hackers gained access to its internal network from where they stole roughly 200 MB of files.

While initially the company didn't reveal the content of these documents, in an updated press release, the company said the files contained primarily information on employees, and not data related to its business dealings and partners.

According to Mitsubishi, the stolen documents contained:

- Data on employment applications for 1,987 people
- The results of a 2012 employee survey that was filled in by 4,566 people from its head office
- Information on 1,569 Mitsubishi Electric workers that retired between 2007 and 2019
- Files with corporate confidential technical materials, sales materials, and others.

The zero-day

This week, Japanese media dug deeper into the hack. According to reports, the hack first originated at a Mitsubishi Electric Chinese affiliate, and then spread to 14 of the company's departments/networks.

The intrusion was allegedly detected after Mitsubishi Electric staff found a suspicious file on one of the company's servers.

None of this was confirmed by the Japanese company, but discovered by Japanese reporters. The only technical detail in relation to the hack Mitsubishi Electric disclosed was the fact that hackers exploited a vulnerability in one of the antivirus products the company was using.

A source with knowledge of the attack told ZDNet that the hackers exploited CVE-2019-18187, a directory traversal and arbitrary file upload vulnerability in the Trend Micro OfficeScan antivirus.

According to a security advisory Trend Micro sent out in October 2019, "affected versions of OfficeScan could be exploited by an attacker utilizing a directory traversal vulnerability to extract files from an arbitrary zip file to a specific folder on the OfficeScan server, which could potentially lead to remote code execution (RCE)."

In a case study on its website, Trend Micro lists Mitsubishi Electric as one of the companies that run the OfficeScan suite.

When it patched CVE-2019-18187 back in October, Trend Micro warned customers that the vulnerability was being actively exploited by hackers in the wild.

Japanese media claimed that the intrusion was the work of a Chinese state-sponsored cyber-espionage group known as Tick.

The Tick hacking group is known for carrying out a large number of hacking campaigns aimed at targets all over the world over the past few years. Currently, it is unclear if the group also used the OfficeScan zero-day against other targets.

Trend Micro declined to comment for this article.

The world's most famous and dangerous APT (state-developed) malware

→

/ security

Do you need antivirus on Linux?

6 ways to protect yourself from getting scammed online, by phone, or IRL

The best VPN free trials for 2024

8 habits of highly se workers

Editorial standards

show comments ↓