CHINESE HACKERS EXPLOITED A TREND MICRO ANTIVIRUS ZERO-DAY USED IN MITSUBISHI ELECTRIC HACK

Pierluigi Paganini January 25, 2020

Chinese hackers have exploited a zero-day vulnerability the Trend Micro OfficeScan antivirus in the recently disclosed hack of Mitsubishi Electric.

According to ZDNet, the hackers involved in the attack against the Mitsubishi Electric have exploited a zero-day vulnerability in Trend Micro OfficeScan to infect company servers.

This week, Mitsubishi Electric disclosed a security breach that might have exposed personal and confidential corporate data. According to the company, attackers did not obtain sensitive information about defense contracts.

RECENT ARTICLES

New Vultur malware version includes enhanced remote control and evasion capabilities

MALWARE / April 01, 2024

Pentagon established the Office of the Assistant Secretary of Defense for Cyber Policy

CYBER WARFARE / April 01, 2024

Info stealer attacks target macOS users

MALWARE / April 01, 2024

Security Affairs newsletter Round 465 by Pierluigi Paganini – INTERNATIONAL EDITION

BREAKING NEWS / March 31, 2024

The breach was detected almost eight months ago, on June 28, 2019, with the delay being attributed to the increased complexity of the investigation caused by the attackers deleting activity logs.

“On June 28, last year, a suspicious behavior was detected and investigated on a terminal in our company, and as a result of unauthorized access by a third party, data was transmitted to the outside,” reads a data breach notification published by the company.

The intrusion took place on June 28, 2019, and the company launched an investigation in September 2019. Mitsubishi Electric disclosed the security incident only after two local newspapers, the Asahi Shimbun and Nikkei, reported the security breach.

Mitsubishi Electric had also already notified members of the Japanese government and Ministry of Defense.

relations at least since 2012,

According to the experts, the group is linked to the People’s Republic of China and is focused on exfiltrating confidential data.

“According to people involved, Chinese hackers Tick may have been involved. According to Mitsubishi Electric, “logs (to check for leaks) have been deleted and it is not possible to confirm whether or not they actually leaked.” reported the Nikkei.

“According to the company, at least tens of PCs and servers in Japan and overseas have been found to have been compromised. The amount of unauthorized access is approximately 200 megabytes, mainly for documents.”

The security breach was discovered after Mitsubishi Electric staff found a suspicious file on one of the company’s servers, further investigation allowed the company to determine that hack of an employee account.

According to the media, hackers gained access to the networks of around 14 company departments, including sales and the head administrative office. Threat actors stole around 200 MB of files including:

- Personal information and recruitment applicant information (1,987)
- New graduate recruitment applicants who joined the company from October 2017 to April 2020, and experienced recruitment applicants from 2011 to 2016 and our employee information (4,566)
- 2012 Survey results regarding the personnel treatment system implemented for employees in the headquarters in Japan, and information on retired employees of our affiliated companies (1,569)

The attackers have exploited a directory traversal and arbitrary file upload vulnerability, tracked as CVE-2019-18187, in the Trend Micro OfficeScan antivirus.

Trend Micro has now addressed the vulnerability, but we cannot exclude that the hackers have exploited the same issue in attacks against other targets. After the security firm patched the CVE-2019-18187 flaw in October, it warned customers that the issue was being actively exploited by hackers in the wild.

“Trend Micro has released Critical Patches (CP) for Trend Micro OfficeScan 11.0 SP1 and XG which resolve an arbitrary file upload with directory traversal vulnerability.” reads the security advisory published by Trend Micro 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). The remote process execution is bound to a web service account, which depending on the web platform used may have restricted permissions. An attempted attack requires user authentication.”

The issue affects OfficeScan versions XG SP1, XG (Non-SP GM build), 11.0 SP1 for Windows.

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

[adrotate banner=”9″]	[adrotate banner=”12″]

Pierluigi Paganini

(SecurityAffairs – Mitsubishi Electric, hacking)

[adrotate banner=”5″]

[adrotate banner=”13″]

APT | China | Hacking | information security news | Mitsubishi Electric | Pierluigi Paganini | Security Affairs | Security News | Trend Micro AV

To contact me write an email to:

Pierluigi Paganini :
pierluigi.paganini@securityaffairs.co

LEARN MORE

QUICK LINKS