Ongoing state cyber espionage campaign via vulnerable edge devices

News item | 10-06-2024 | 12:00

Earlier this year, the NCSC, together with the Military Intelligence and Security Service (MIVD) and the General Intelligence and Security Service (AIVD), published a report on the advanced COATHANGER malware targeting FortiGate systems. Since then, the MIVD has conducted further investigation and has shown that the Chinese cyber espionage campaign appears to be much more extensive than previously known. The NCSC therefore calls for extra attention to this campaign and the abuse of vulnerabilities in edge devices. For this purpose, the NCSC has drawn up a knowledge product with additional information about edge devices, associated challenges and measures to be taken.

The wider COATHANGER campaign

Since the publication in February, the MIVD has continued to investigate the broader Chinese cyber espionage campaign. This revealed that the state actor gained access to at least 20,000 FortiGate systems worldwide within a few months in both 2022 and 2023 through the vulnerability with the characteristic CVE-2022-42475 . Furthermore, research shows that the state actor behind this campaign was already aware of this vulnerability in FortiGate systems at least two months before Fortinet announced the vulnerability. During this so-called 'zero-day' period, the actor alone infected 14,000 devices. Targets include dozens of (Western) governments, international organizations and a large number of companies within the defense industry.

The state actor installed malware at relevant targets at a later date. This gave the state actor permanent access to the systems. Even if a victim installs security updates from FortiGate, the state actor continues to have this access.

It is not known how many victims actually have malware installed. The Dutch intelligence services and the NCSC consider it likely that the state actor could potentially expand its access to hundreds of victims worldwide and carry out additional actions such as stealing data.

Even with the technical report on the COATHANGER malware, infections from the actor are difficult to identify and remove. The NCSC and the Dutch intelligence services therefore state that it is likely that the state actor still has access to systems of a significant number of victims.

Mitigation measures when using edge devices

The NCSC and the Dutch intelligence services have been seeing a trend for some time that vulnerabilities in publicly accessible edge devices such as firewalls, VPN servers, routers and email servers are being exploited. Due to the security challenges of edge devices, these devices are a popular target for malicious parties. Edge devices are located at the edge of the IT network and regularly have a direct connection to the internet. In addition, these devices are often not supported by Endpoint Detection and Response (EDR) solutions.

Initial compromise of an IT network is difficult to prevent if the attacker uses a zero-day. It is therefore important that organizations apply the 'assume breach' principle. This principle states that a successful digital attack has already taken place or will soon take place. Based on this, measures are taken to limit the damage and impact. This includes taking mitigating measures in the areas of segmentation, detection, incident response plans and forensic readiness .

The NCSC knowledge product 'Dealing with edge devices' describes further challenges and digital threats when using edge devices and offers specific perspectives for action for organizations per challenge.

Knowledge product 'Dealing with edge devices'

- **Factsheet Dealing with edge devices**

  Contemporary organizations often use edge devices. These systems are located at the edge of the network and consist...

  Fact sheet | 10-06-2024