Check Point response to MysterySnail vulnerability

Archived: 2026-04-05 14:42:30 UTC

ProductAnti-Bot, Anti-Virus, Harmony Endpoint, IPS, Threat Emulation

VersionAll

Last Modified2021-10-20

Solution

On October 13, 2021, details of an exploitation of a vulnerability in Microsoft Windows named "MysterySnail" became publicly known. Microsoft patched the vulnerability in its October 2021 Patch Tuesday.

The CVE assigned to the vulnerability is CVE-2021-40449.

"MysterySnail" is a remote shell access Trojan installed on compromised Windows servers. "MysterySnail" has privilege escalation, advanced persistence, and data-stealing capabilities. It was recently found at the end of an exploit chain attack campaign by Chinese APT “IronHusky”.

Check Point provides security coverage from the vulnerability with these Threat Prevention protections:

- **IPS**

Microsoft Win32k Elevation of Privilege (CVE-2021-40449)

- **Anti-Bot**

MysterySnail.TC.[X]

- **Anti-Virus**

RAT.Win32.MysterySnail.TC.[X]

- **Threat Emulation**

KAV-Trojan.Win64.Agentb.[X]
RAT.Wins.MysterySnail.A

- **Harmony Endpoint**

RAT.Win.MysterySnail.B
RAT.Win.MysterySnail.C

Article Properties

Access LevelGeneral

StatusApproved

Date Created2021-10-14

Last Modified2021-10-20
