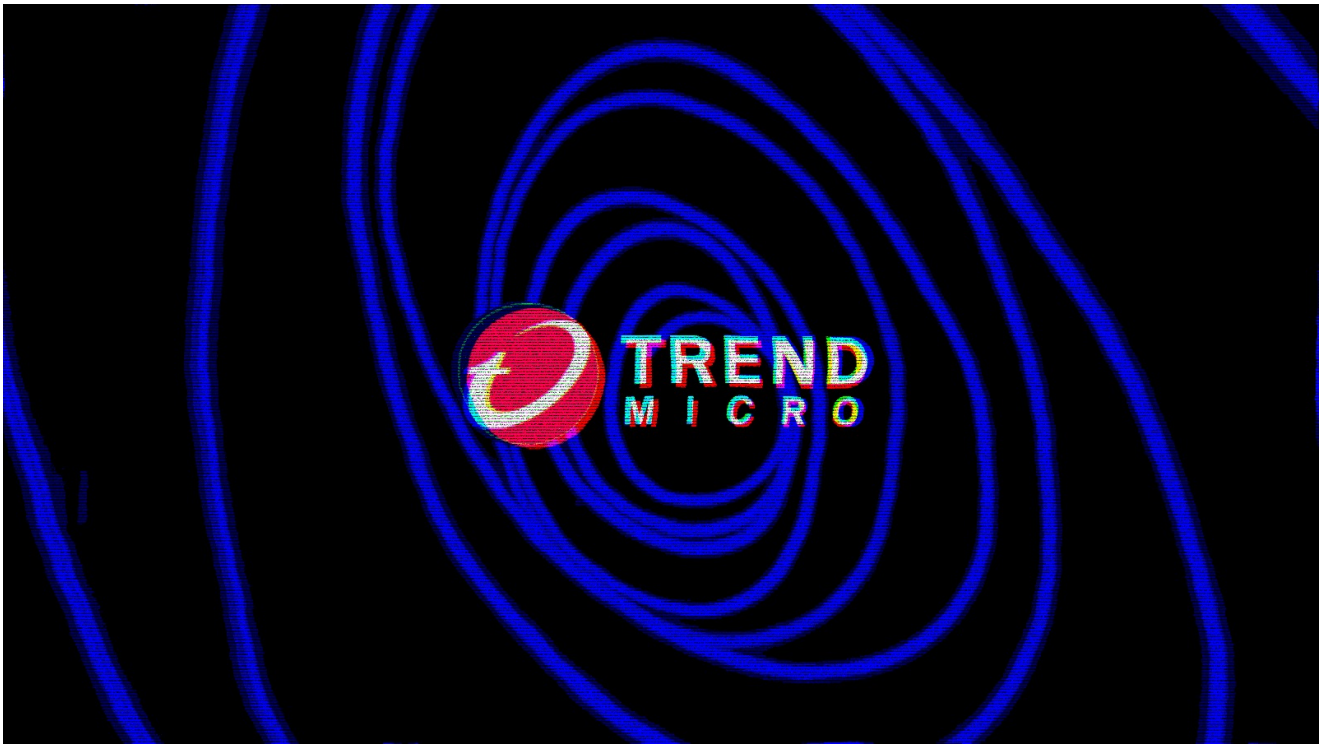
Trend Micro warns of actively exploited Apex One RCE vulnerability

bleepingcomputer.com/news/security/trend-micro-warns-of-actively-exploited-apex-one-rce-vulnerability/

Sergiu Gatlan

By
Sergiu Gatlan

- September 13, 2022
- 10:48 AM
- 0



Security software firm Trend Micro warned customers today to patch an actively exploited Apex One security vulnerability as soon as possible.

Apex One is an endpoint security platform that provides businesses with automated threat detection and response against malicious tools, malware, and vulnerabilities.

This flaw (CVE-2022-40139) enables attackers to execute arbitrary code remotely on systems running unpatched software.

"Improper validation of some components used by the rollback mechanism in Trend Micro Apex One and Trend Micro Apex One as a Service clients could allow a Apex One server administrator to instruct affected clients to download an unverified rollback package, which

could lead to remote code execution," the company explained in a security advisory published today.

Luckily, threat actors must first obtain access to the Apex One server administration console to exploit this bug successfully.

Even though this definitely raises the skill level required to abuse CVE-2022-40139 in attacks, Trend Micro warned customers today that it has already observed at least one active exploitation attempt in the wild.

"Trend Micro has observed at least one active attempt of potential exploitation of this vulnerability in the wild. Customers are strongly encouraged to update to the latest versions as soon as possible," the company said.

Users should immediately update their installation to the latest version, Apex One Service Pack 1 (Server Build 11092 and Agent Build 11088).

Authentication bypass bug also fixed today

Today, Trend Micro addressed another high severity vulnerability in the Apex One product (CVE-2022-40144), allowing potential attackers to bypass authentication by falsifying request parameters on affected installations.

"Exploiting these type of vulnerabilities generally require that an attacker has access (physical or remote) to a vulnerable machine. However, even though an exploit may require several specific conditions to be met, Trend Micro strongly encourages customers to update to the latest builds as soon as possible," Trend Micro added.

"In addition to timely application of patches and updated solutions, customers are also advised to review remote access to critical systems and ensure policies and perimeter security is up-to-date."

In April, the security software vendor fixed another actively exploited security flaw in the Apex Central product management console that let remote attackers execute arbitrary code on compromised systems.

CISA later added the bug to its Known Exploited Vulnerabilities catalog, requiring federal civilian agencies to patch the actively used Apex Central bug within the next three weeks, until April 21, 2022.

Related Articles:

Hackers exploit critical Juniper RCE bug chain after PoC release

Hackers exploit BleedingPipe RCE to target Minecraft servers, players

Microsoft: Unpatched Office zero-day exploited in NATO summit attacks

300,000+ Fortinet firewalls vulnerable to critical FortiOS RCE bug

Exploit released for Juniper firewall bugs allowing RCE attacks