Microsoft says Iranian hackers are exploiting the Zerologon vulnerability

By Written by Catalin Cimpanu, ContributorContributor Oct. 5, 2020 at 4:50 p.m. PT

Archived: 2026-04-05 15:34:40 UTC

Microsoft said on Monday that Iranian state-sponsored hackers are currently exploiting the Zerologon vulnerability in real-world hacking campaigns.

Successful attacks would allow hackers to take over servers known as domain controllers (DC) that are the centerpieces of most enterprise networks and enable intruders to gain full control over their targets.

The Iranian attacks were detected by Microsoft's Threat Intelligence Center (MSTIC) and have been going on for at least two weeks, the company said today in a short tweet.

> MSTIC has observed activity by the nation-state actor MERCURY using the CVE-2020-1472 exploit (ZeroLogon) in active campaigns over the last 2 weeks. We strongly recommend patching. Microsoft 365 Defender customers can also refer to these detections: https://t.co/ieBj2dox78
>
> — Microsoft Security Intelligence (@MsftSecIntel) October 5, 2020

MSTIC linked the attacks to a group of Iranian hackers that the company tracks as **MERCURY**, but who are more widely known under their monicker of MuddyWatter.

The group is believed to be a contractor for the Iranian government working under orders from the Islamic Revolutionary Guard Corps, Iran's primary intelligence and military service.

According to Microsoft's Digital Defense Report, this group has historically targeted NGOs, intergovernmental organizations, government humanitarian aid, and human rights organizations.

Nonetheless, Microsoft says that Mercury's most recent targets included "a high number of targets involved in work with refugees" and "network technology providers in the Middle East."

Attacks began after public Zerologon PoC

Zerologon was described by many as the most dangerous bug disclosed this year. The bug is a vulnerability in Netlogon, the protocol used by Windows systems to authenticate against a Windows Server running as a domain controller.

Exploiting the Zerologon bug can allow hackers to take over an unpatched domain controller, and inherently a company's internal network.

Attacks usually need to be carried out from internal networks, but if the domain controller is exposed online, they can also be carried out remotely over the internet.

Microsoft issued patches for Zerologon (CVE-2020-1472) in August, but the first detailed write-up about this bug was published in September, delaying most of the attacks.

But while security researchers delayed publishing details to give system administrators more time to patch, weaponized proof-of-concept code for Zerologon was published almost on the same day as the detailed write-up, spurring a wave of attacks within days.

Following the bug's disclosure, DHS gave federal agencies three days to patch domain controllers or disconnect them from federal networks in order to prevent attacks, which the agency was expecting to come -- and they did, days later.

> Microsoft is actively tracking threat actor activity using exploits for the CVE-2020-1472 Netlogon EoP vulnerability, dubbed Zerologon. We have observed attacks where public exploits have been incorporated into attacker playbooks.
>
> — Microsoft Security Intelligence (@MsftSecIntel) September 24, 2020

The MERCURY attacks appear to have begun around one week after this proof-of-concept code was published, and around the same time, Microsoft began detecting the first Zerologon exploitation attempts.

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

Security

Editorial standards
