Hackers are using a severe Windows bug to backdoor unpatched servers

Getty Images

reader comments

2 with 2 posters participating

Share this story

One of the most critical Windows vulnerabilities disclosed this year is under active attack by hackers who are trying to backdoor servers that store credentials for every user and administrative account on a network, a researcher said on Friday.

Zerologon, as the vulnerability has been dubbed, gained widespread attention last month when the firm that discovered it said it could give attackers instant access to active directories, which admins use to create, delete, and manage network accounts. Active directories and the domain controllers they run on are among the most coveted prizes in hacking because once hijacked, they allow attackers to execute code in unison on all connected machines. Microsoft patched CVE-2020-1472, as the security flaw is indexed, in August.

On Friday, Kevin Beaumont, working in his capacity as an independent researcher, said in a blog post that he had detected attacks on the honeypot he uses to keep abreast of attacks hackers are using in the wild. When his lure server was unpatched, the attackers were able to use a powershell

script to successfully change an admin password and backdoor the server.

Something more problematic than sophisticated

In an interview, Beaumont said that the attack appeared to be entirely scripted, with all commands being completed within seconds. With that, the attackers installed a backdoor allowing remote administrative access to devices inside his mock network. The attackers—who set up an account with the username sdb and the password jinglebell110@—also enabled Remote Desktop. As a result, the attackers would continue to have remote access if CVE-2020-1472 is later patched.

“The takeaway for me is attackers are spraying the Internet to provide backdoors into unpatched Active Directory systems in an automated fashion,” Beaumont told Ars. “That isn’t great news. It’s not super sophisticated, but these attackers are doing something effective—which is usually more problematic.”

Friday’s findings are the most detailed yet about in-the-wild attacks that exploit the critical vulnerability. Late last month and again earlier this month Microsoft warned that Zerologon was under active attack by hackers, some or all of them part of a threat group dubbed Mercury, which has ties to the Iranian government. A few weeks ago, Beaumont’s honeypot also detected exploit attempts.

Researchers gave the vulnerability the name Zerologon because attacks work by sending a string of zeros in a series of messages that use the Netlogon protocol, which Windows servers rely on for a variety of tasks, including allowing end users to log in to a network.

People with no authentication can use the exploit to gain domain administrative credentials, as long as the attackers

have the ability to establish TCP connections with a vulnerable domain controller. In some cases, attackers may use a separate vulnerability to gain a foothold inside a network and then exploit Zerologon to take over the domain controller, the Department of Homeland Security's cybersecurity arm—the Cybersecurity and Infrastructure Security Agency—said last Friday. The agency said exploits were threatening government-controlled election systems.

To be effective, honeypots generally must let down defenses that are standard on many networks. In that sense, they can give a one-sided view of what's happening in the real world. Beaumont's results are nevertheless illustrative both of the effectiveness of current Zerologon attacks and the concerning results they achieve.

https://arstechnica.com/?p=1715441