Feds issue emergency order for agencies to patch critical Windows flaw

reader comments

61 with 49 posters participating, including story author

Share this story

The US Department of Homeland Security is giving federal agencies until midnight on Tuesday to patch a critical Windows vulnerability that can make it easy for attackers to become all-powerful administrators with free rein to create accounts, infect an entire network with malware, and carry out similarly disastrous actions.

Zerologon, as researchers have dubbed the vulnerability, allows malicious hackers to instantly gain unauthorized control of the Active Directory. An Active Directory stores data relating to users and computers that are authorized to use email, file sharing, and other sensitive services inside large organizations. Zerologon is tracked as CVE-2020-1472. Microsoft published a patch last Tuesday.

An unacceptable risk

The flaw, which is present in all supported Windows server versions, carries a critical severity rating from Microsoft as well as a maximum of 10 under the Common Vulnerability Scoring System. Further raising that stakes was the release by multiple researchers of proof-of-concept exploit code that

could provide a roadmap for malicious hackers to create working attacks.

Officials with the Cybersecurity and Infrastructure Security Agency, which belongs to the DHS, issued an emergency directive on Friday that warned of the potentially severe consequences for organizations that don't patch. It states:

> *CISA has determined that this vulnerability poses an unacceptable risk to the Federal Civilian Executive Branch and requires an immediate and emergency action. This determination is based on the following:*
>
> - *the availability of the exploit code in the wild increasing likelihood of any unpatched domain controller being exploited;*
> - *the widespread presence of the affected domain controllers across the federal enterprise;*
> - *the high potential for a compromise of agency information systems;*
> - *the grave impact of a successful compromise; and*
> - *the continued presence of the vulnerability more than 30 days since the update was released.*

CISA, which has authorization to issue emergency directives intended to mitigate known or suspected security threats, is giving organizations until 11:59pm EDT on Monday to either install a Microsoft patch or disconnect the vulnerable domain controller from the organization network.

No later than 11:59pm EDT on Wednesday, agencies are to submit a completion report attesting the update has been applied to all affected servers or provide assurance that newly provisioned or previously disconnected servers will be patched.

Exploitation is easier than expected

When details of the vulnerability first surfaced last Tuesday, many researchers assumed it could be exploited only when attackers already had a toehold inside a vulnerable network, by either a malicious insider or an outside attacker who had already gained lower-level user privileges. Such post-compromise exploits can be serious, but the requirement can be a high-enough bar to either buy vulnerable networks time or push attackers into exploiting easier but less severe security flaws.

Since then, several researchers have said that it's possible for attackers to exploit the vulnerability over the Internet without first having such low-level access. The reason: despite the risks, some organizations expose their domain controllers—that is, the servers that run Active Directory—to the Internet. Networks that do this and also have exposed Server Message Block for file sharing or Remote Procedure Call for intra-network data exchange may be exploitable with no other requirements.

"If you have set up detections for #zerologon (CVE-2020-1472), don't forget that it could also be exploited over SMB!" researchers from security firm Zero Networks wrote. Run this test script (based on @SecuraBV) for both RPC/TCP and RPC/SMB."

Kevin Beaumont, acting in his capacity as an independent researcher, added: "There's a good (but minor) barrier to entry as so far the exploits don't automate remotely querying the domain and Netbios name of DC. One unpatched domain controller = every patched domain endpoint is vulnerable to RCE. Another pivot, if you have SMB open—RPC over SMB. Attn network detection folks."

> *Another pivot, if you have SMB open — RPC over SMB. Attn network detection folks.* *https://t.co/2np1gLgTfk*
>
> *— Kevin Beaumont (@GossiTheDog)* *September 17, 2020*

Queries using the Binary Edge search service show that almost 30,000 domain controllers are viewable and another 1.3 million servers have RPC exposed. In the event either of these settings apply to a single server, it may be vulnerable to remote attacks that send specially crafted packets that give full access to the active directory.

Beaumont and other researchers continue to find evidence that people are actively developing attack code, but so far there are no public reports that exploits—either successful or attempted—are active. Given the stakes and the amount of publicly available information about the vulnerability, it wouldn't be surprising to see in-the-wild exploits emerge in the coming days or weeks.

https://arstechnica.com/?p=1708395