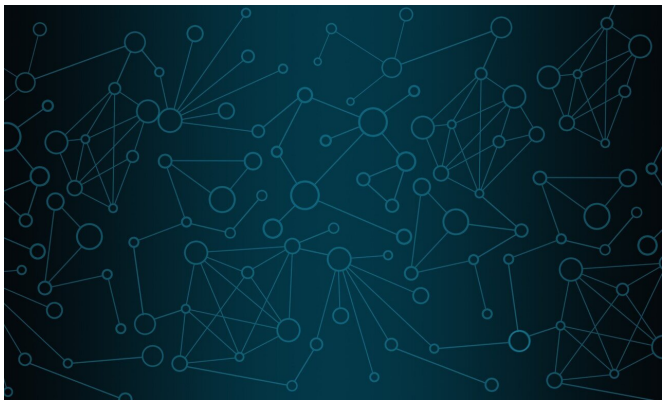
Zerologon: Microsoft addressing severe network exploit

15 September 2020, by Peter Grad



Credit: Pixabay/CC0 Public Domain

A Dutch security firm reported last week that it uncovered a severe Windows vulnerability last month that allowed hackers to take over network administrator privileges with a single click.

The security firm, Secura, said Microsoft was notified of the problem and issued the first of two patches in August. The second patch, a more comprehensive solution, is slated for February 2021.

"The attack has a huge impact," Secura's security expert Tom Tervoort said in company white paper. "It basically allows any attacker on the local network (such as a malicious insider or someone who simply plugged in a device to an on-premise network port) to completely compromise the Windows domain."

Experts view the vulnerability, called Zerologon, as one of the most severe ever to hit Microsoft. It was assigned a score of 10/10, the highest degree of severity under the Common Vulnerability Scoring System.

Tervoort said the exploit takes advantage of a faulty cryptographic algorithm employed during the Windows Server Netlogon authentication process. In doing so, the attacker can masquerade as the owner of any computer on a network during authentication, disable security functions and alter or delete passwords.

Experts say it would be a likely approach that attackers inserting ransomware and other malware would favor. It provides easy entry into an unlimited number of affiliated computers on a network. All it takes is a single employee to click on a hostile email attachment or link for an entire network to be compromised.

Tervoort said the entire attack takes no more than three seconds to execute.

Secura researchers waited to release a copy of the exploit for IT administrators to study until after wide release of Microsoft's patch.

"Customers who apply the update, or have automatic updates enabled, will be protected," Microsoft said. The updates work "by modifying how Netlogon handles the usage of Netlogon secure channels."

IT administrators are cautioned that hackers conceivably could examine the first Microsoft patch and work backwards to to devise an alternate line of attack.

With the 2021 fix, Microsoft will require revised logon protocols and updating of all equipment connected to networks. Equipment that is not updated to the more secure protocols must be whitelisted.

Secura has released a python script that can alert IT administrators to any breach by Zerologon.

Zerologon's name stems from the use of a string of zeros to fill out various fields during a Netlogon

connection.

"By simply sending a number of Netlogon messages in which various fields are filled with zeros, an attacker can change the computer password of the domain controller that is stored in the AD. This can then be used to obtain domain admin credentials and then restore the original DC password," Secura researchers said.

One small consolation for IT administrators is that a hacker must already be on the network to launch an attack. Zerologon cannot be executed from outside the network.

More information:
www.secura.com/blog/zero-logon

portal.msrc.microsoft.com/en-U …
visory/CVE-2020-1472

APA citation: Zerologon: Microsoft addressing severe network exploit (2020, September 15) retrieved 12 August 2022 from https://techxplore.com/news/2020-09-zerologon-microsoft-severe-network-exploit.html