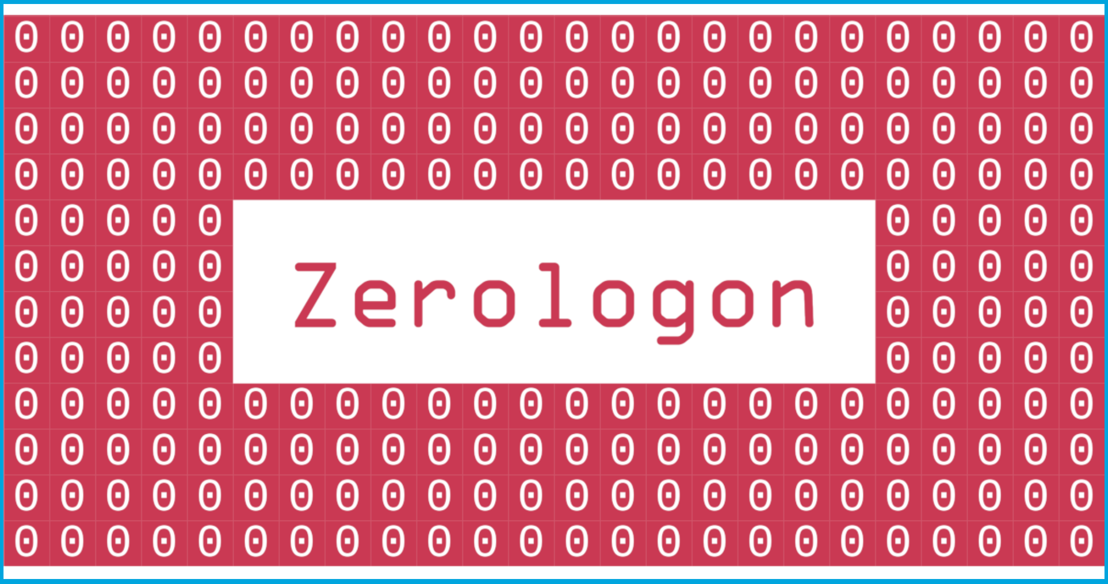
kindred

Security Newsletter

21 September 2020

Subscribe to this newsletter

Zerologon attack lets hackers take over enterprise networks: Patch now



Last month Microsoft patched one of the most severe bugs ever reported to the company, an issue that could be abused to easily take over Windows Servers running as domain controllers in enterprise networks.

The bug was patched in the August 2020 Patch Tuesday under the identifier of CVE-2020-1472. It was described as an elevation of privilege in Netlogon, the protocol that authenticates users against domain controllers. The vulnerability received the maximum severity rating of 10, but details were never made public, until now. The entire attack is very fast and can last up to three seconds, at most.There are limitations to how a Zerologon attack can be used. For starters, it cannot be used to take over Windows Servers from outside the network. An attacker first needs a foothold inside a network. However, when this condition is met, it's literally game over for the attacked company. Furthermore, this bug is also a boon for malware and ransomware gangs, which often rely on infecting one computer inside a company's network and then spreading to multiple others. With Zerologon, this task has been considerably simplified.

Attacks using Zerologon are a given, primarily due to the bug's severity, wide impact, and benefits for attackers. Since the release of Secura's writeup, numerous researchers have released proof-of-concept exploits that allow a user to gain domain administrator privileges on a vulnerable network. As fixing the Zerologon vulnerability can cause some devices to not properly authenticate, Microsoft is rolling out the fix in two stages. The first stage was released on August 11th in the form of a security update that will prevent Windows Active Directory Domain controllers from using unsecured RPC communication. On February 9th, 2021, as part of the Patch Tuesday updates, Microsoft will release a second update that will enter the enforcement phase that requires all devices on the network to use secure-RPC, unless specifically allowed by an administrator.

Read More on ZDNet

Even More on BleepingComputer

First death reported following a ransomware attack on a German hospital

On September 10th, the University Hospital Düsseldorf (UKD) in Germany suffered a ransomware attack. The patient, identified only as a woman who needed urgent medical care, died after being re-routed to a hospital in the city of Wuppertal, more than 30 km away from her initial intended destination, the Duesseldorf University Hospital. The threat actors compromised the hospital's network through a known software vulnerability in Citrix ADC. Patches for the Citrix ADC vulnerability have been available since January 2020.

With their IT systems disrupted, the hospital announced that planned and outpatient treatments and emergency care could not occur at the hospital. Those seeking emergency care were instead redirected to more distant hospitals for treatment. A patient in a life-threatening condition was redirected to a more distant hospital in Wuppertal after University Hospital Düsseldorf deregistered its emergency services. This disruption led to the patient receiving care an hour later, which may have led to her death.

German media reports that the police contacted the ransomware operators via the ransom note instructions and explained that their target was a hospital. The ransom notes left on the hospital's encrypted servers were incorrectly addressed to Heinrich Heine University, rather than the hospital itself. After the police contacted the threat actors and explained that they encrypted a hospital, the ransomware operators withdrew the ransom demand and provided a decryption key.

Read More on ZDNet

Even More on BleepingComputer

More #News

- Dunkin' Data Breach Settlement Paves the Way for More Suits
- Android 11 — 5 New Security and Privacy Features, including One-time permissions
- Hands on with iOS 14's new data breach notification feature
- Zoom adds two-factor authentication (2FA) support to all accounts
- More Details Emerge on Operations, Members of Chinese Group APT41
- Mozilla shuts down Firefox Send and Firefox Notes services
- How ransomware operators are joining forces to carry out attacks
- Payment Card Skimming Hits 2,000 E-Commerce Site
- New 'BLESA' Bluetooth security flaw

#Patch Time!

- CVE-2020-1472 "Zerologon" Critical Privilege Escalation: What You Need To Know
- How to patch CentOS against BootHole
- Adobe out-of-band patch released to tackle Media Encoder vulnerabilities
- Information Disclosure, XSS Vulnerabilities Patched in Drupal

#Tech and #Tools

- Zerologon – hacking Windows servers with a bunch of zeros
- Hacking on Bug Bounties for Four Years
- Quantifying Threat Actors with Threat Box
- Application-level Purple Teaming: A case study
- CrowdStrike's 2020 threat report
- How A Cryptocurrency Miner Made Its Way onto Our Internal Kubernetes Clusters
- Windows Lateral Movement Part 2 – DCOM
- WMIHACKER: lateral movement command execution test tool
- Attacking SIEM with Fake Logs
- ZeroLogon testing script
- A Year and a Half of End-to-End Encryption at Misakey
- Detections of Past, Present, and Future
- Microsoft Releases Open Source Fuzzing Framework for Azure

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us