What Is Zerologon and How Do You Mitigate It?

blog.netwrix.com/2023/04/14/zerologon

Kevin Joyce

Commonly referred to as Zerologon, CVE-2020-1472 is the Common Vulnerabilities and Exposures (CVE) identifier assigned to a vulnerability in Microsoft's Netlogon Remote Protocol (MS-NRPC). MS-NRPC is essential for authentication of both user and machine accounts in Active Directory.

The Zerologon vulnerability is a flaw in the cryptographic authentication scheme used by Netlogon that can enable an attacker to bypass authentication and gain administrator-level privileges to a computer — including a domain controller (DC). Essentially, an unauthenticated attacker can use the Netlogon Remote Protocol to connect to a DC and change its password to the value of their choice, including an empty value. Since the attack requires no authentication and only network access, it has been assigned a CVSS score of 10.0 (critical). This is the highest score possible.

Timeline for Addressing the Zerologon Attack Vulnerability

In August 2020, Microsoft released a patch to address the vulnerability, along with controls to aid in monitoring and mitigating attacks. On September 11, 2020, Secura publicly announced the vulnerability, dubbed Zerologon, in their blog and posted some initial proof of concept code to GitHub.

In addition to the patch release for CVE-2020-1472, Microsoft created a rollout strategy that comprised two phases: deployment and enforcement. Both phases are now complete.

Phase 1: Deployment Phase

The patch released by Microsoft in August of 2020 began the deployment phase, which also included the following:

· Enforcement of secure RPC usage for machine accounts on Windows-based devices, trust accounts, and Windows and non-Windows DCs

· A new Group Policy: Domain controller: Allow vulnerable Netlogon secure channel connections

· A new registry key: FullSecureChannelProtection

· New events for Netlogon connections

Details on the new Group Policy, registry key and events are provided below.

The deployment strategy was as follows:

1. Patch all DCs in the forest.
2. Monitor the new events and then ensure that applications and machines making vulnerable connections are updated if possible and exceptions are made in the Group Policy setting for applications or machines cannot be updated.
3. If the steps above are completed, enable the enforcement mode registry key ahead of the enforcement phase described below.

Details of the Group Policy

The new Group Policy, “Domain controller: Allow vulnerable Netlogon secure channel connections,” was designed to serve as a temporary measure for third-party devices as updates were deployed. It has the following two values:

· **Allow** — The domain controller will allow the specified groups or accounts to use a Netlogon secure channel without secure RPC.

· **Deny** — This setting is the same as the default behavior: The domain controller will require the specified groups or accounts to use a Netlogon secure channel with secure RPC.

Details of the Registry Setting

The path for the registry setting is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
```

The setting, FullSecureChannelProtection, has two possible values:

· **0** (default during this phase) — Allows for vulnerable Netlogon secure channel connections from non-Windowsdevices

· **1** (enforcement mode) — Domain controllers will deny all vulnerable connections unless the account is specified in the new Group Policy described above.

Details on New Windows Events

Microsoft released the following events to aid support teams during the enforcement phase:

· **Events 5827 & 5828** — These events are logged when connections involve a device running a non-supported version of Windows; it is also possible for non-Windows devices to trigger the events.

· **Events 5830 and 5831** — These events are logged when connections are allowed, but only because of the Group Policy configuration.

· **Event 5829** — This event is logged when connections are allowed, but only because enforcement mode is not in effect.

Phase 2: Enforcement Phase

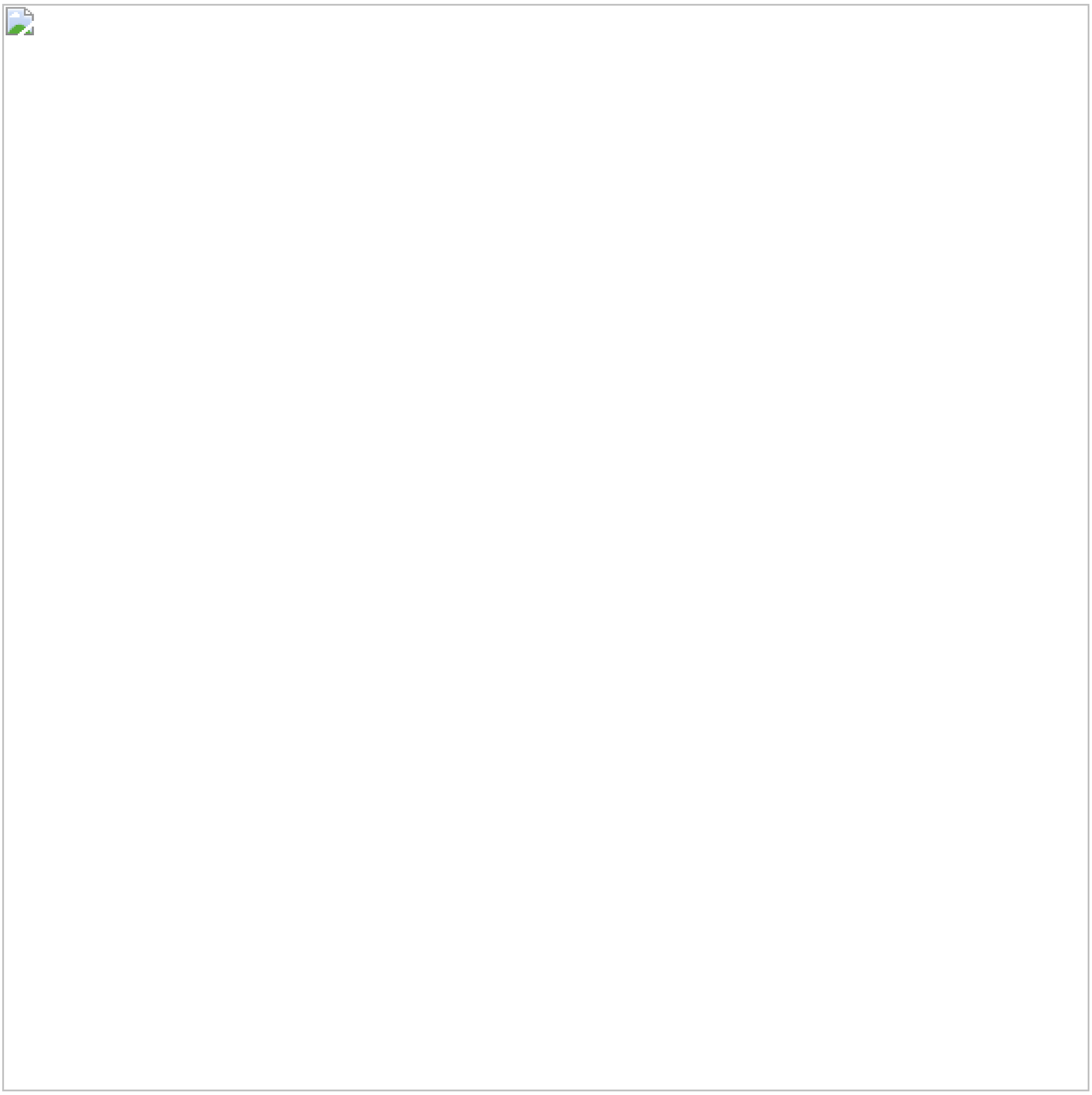
This phase began in February 2021. It enforces secure RPC usage for machine accounts on non-Windows based devices unless they are explicitly configured in the new Group Policy. At that point, the FullSecureChannelProtection registry key was no longer needed and event 5829 was retired.

How Did Zerologon Attacks Word?

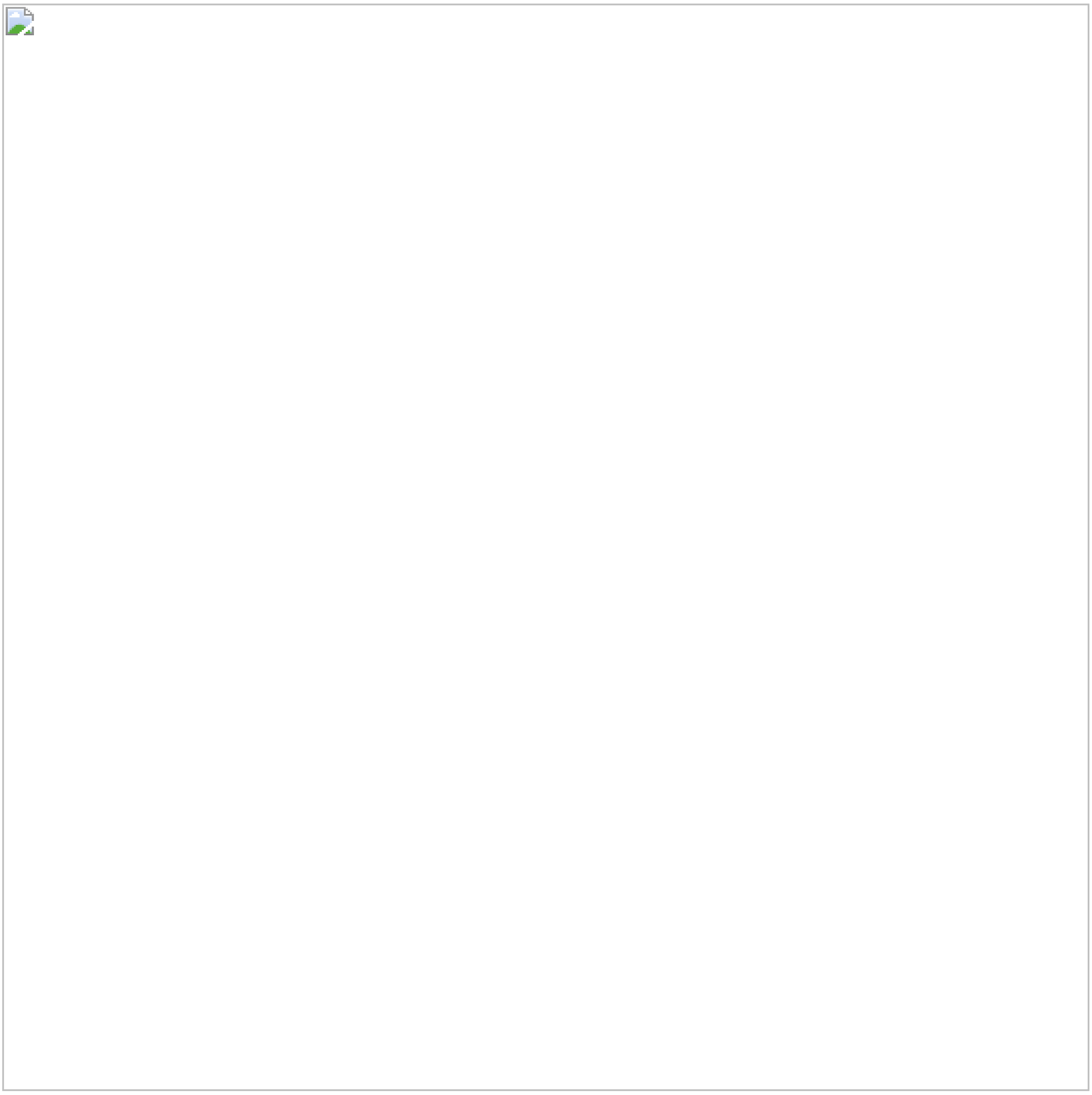
The Zerologon vulnerability allowed a malicious actor on a network to take over a domain controller or even an entire domain. Here is how an adversary could use Mimikatz to execute a Zerologon attack:

1. First, the adversary determines whether a target domain controller is vulnerable to the Zerologon exploit by running this command:

```
lsadump::Zerologon /target:sbpmlab-dc3 /account:sbpmlab-dc3$ /null /ntlm
```

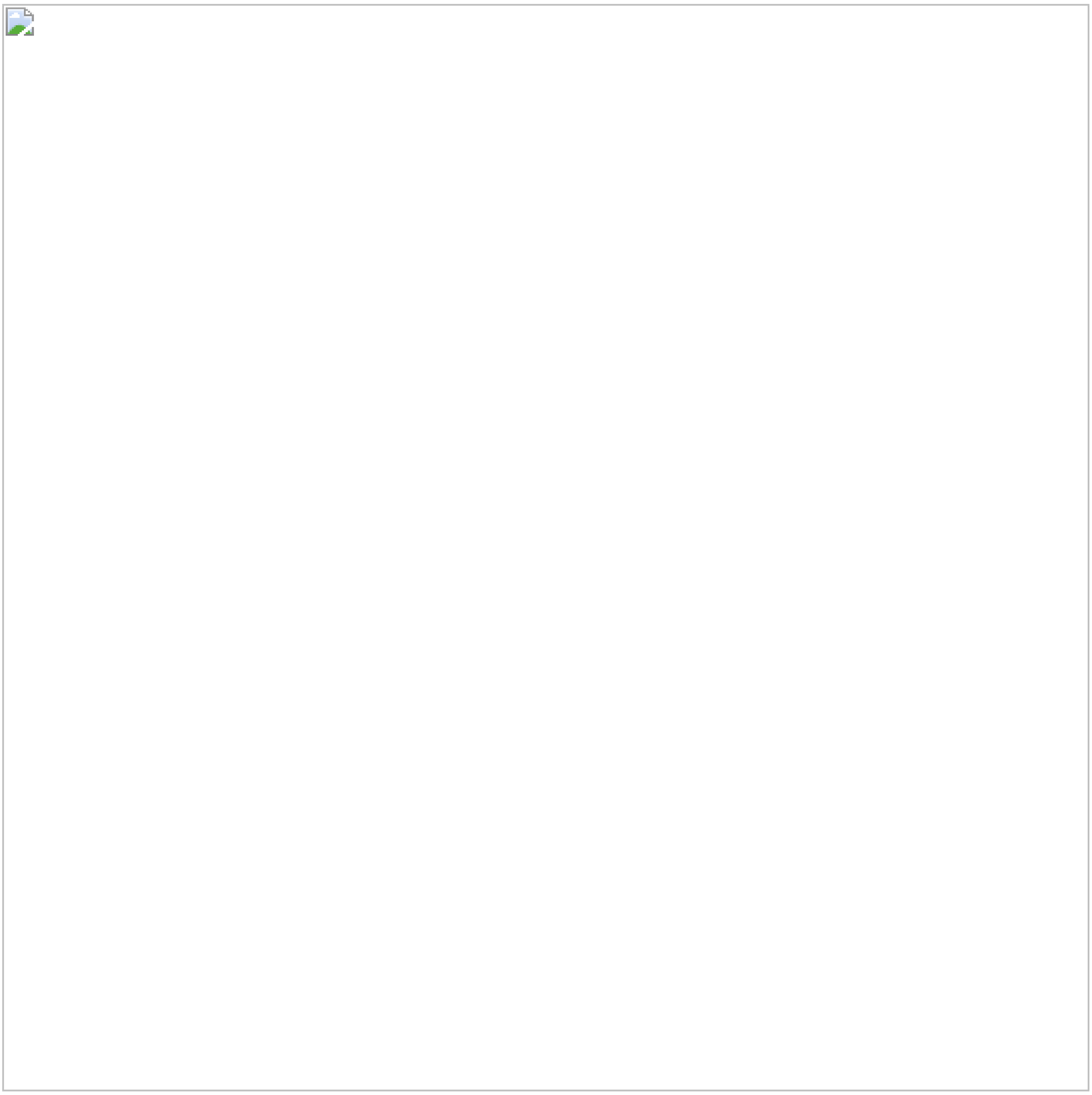


When the adversary finds a vulnerable DC, they run the same command but add **/exploit** to exploit the vulnerability and change the DC’s password to an empty string:



Once the password has been reset, the attacker can use Mimikatz to run a DCSync attack to get the hash of either a Domain Admin account or the KRBTGT account:

```
lsadump::dcsync /domain:sbpmlab.net /dc:sbpmlab-dc3 /user:krbtgt
/authuser:sbpmlab-dc3$ /authdomain:sbpmlab /authpassword:”” /authntlm
```



How Netwrix Can Help

As you can see, it is alarmingly easy for a malicious actor who has gained a foothold in your network to find an unpatched domain controller and execute a Zerologon attack. Netwrix offers two solutions that can help you mitigate your risk.

Analyze and Mitigate Zerologon Risk with Netwrix StealthAUDIT

Netrix StealthAUDIT helps you ensure you have taken the necessary steps to fortify your IT ecosystem against Zerologon attacks. In particular, it provides two reports that provide actionable information on the status of your domain controllers and the events and traffic on those domain controllers.

Reviewing Domain Controller Status

The following information helps you determine whether each of your domain controllers has received the August 2020 patch and whether it is in enforcement mode:

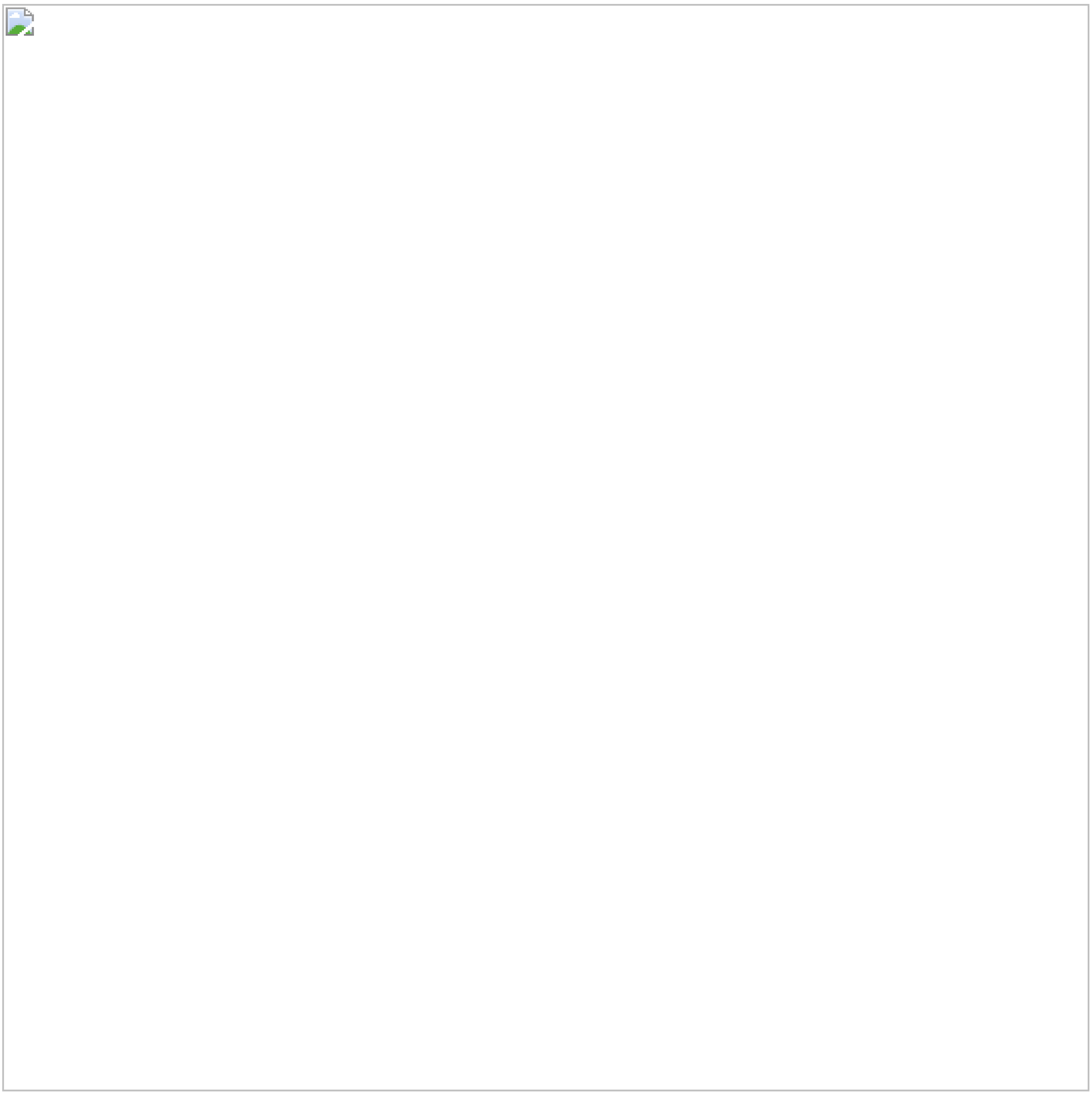
· The FullSecureChannelProtection registry key value

- The last reboot time
- The last patch install date for the machine

Here is a sample report:

Checking Group Policy Settings

Netwrix StealthAUDIT also reports on the configuration of the new Group Policy, “Domain controller: Allow vulnerable Netlogon secure channel connections” so you can see which *domain controllers* are exempted from the policy. A sample report is shown below.



Spotting Empty Domain Controller Passwords

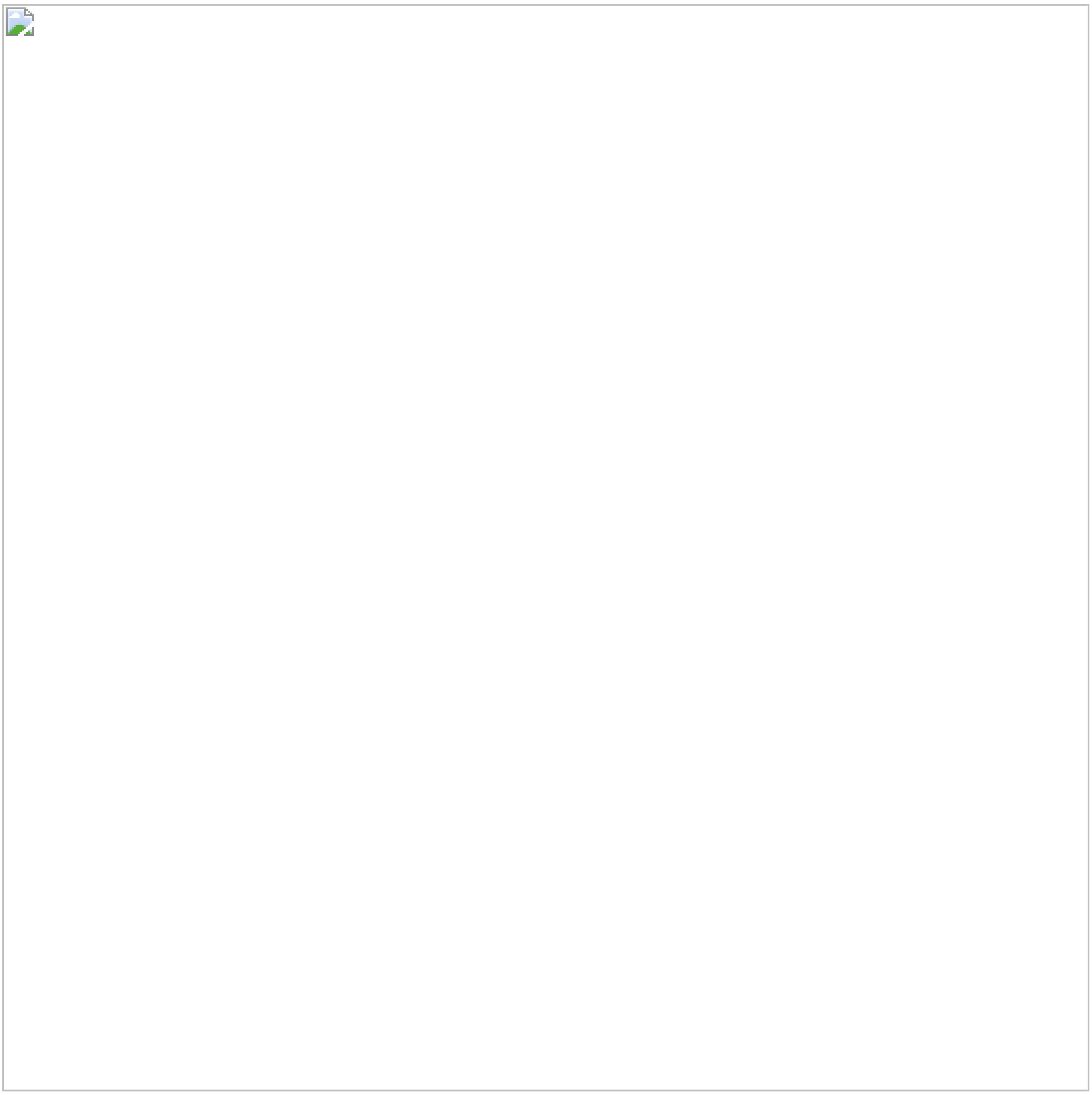
An empty password on a domain controller can indicate that a Zerologon attack has taken place. Whatever the cause, an empty DC password is extremely risky and should be rectified promptly.

Analyzing Event Logs

Netwrix StealthAUDIT also examines all the event IDs associated with the August patch, including events 5827, 5828, 5829, 5830 and 5831. This report helps administrators understand the type of traffic in their environment and its frequency. Most importantly, it identifies the accounts that are creating 5829 events. Those accounts must either be updated or specified as exceptions in the new Group Policy.

Spot Zerologon Attacks with Netwrix Threat Manager

Netwrix Threat Manager can detect and respond to abnormal behavior and advanced threats, including Zerologon, with high accuracy and speed. The screenshot below shows an example of a detected Zerologon attack:



Conclusion

The Zerologon vulnerability received the maximum CVSS score for good reason — exploiting it enables an adversary to gain control of domain controllers, which are vital to authentication and authorization in your IT ecosystem. Accordingly, even if you think you have completed the two-phase mitigation process laid out by Microsoft, it is wise to remain vigilant. Be sure to check the status of your DCs, watch for signs of active exploits, and have the power to shut them down automatically before your business suffers a breach or downtime.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.