



# Detecting the ZeroLogon vulnerability in LogPoint

September 21st, 2020 - 3 min read

**By Bhabesh Raj Rai, Associate Security Analytics Engineer, LogPoint**

On August 11, 2020, [Microsoft released a security advisory for CVE-2020-1472](#), with a CVSS score of 10, a critical privilege escalation flaw when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller; using the Netlogon Remote Protocol (MS-NRPC). What makes this flaw critical is that an unauthenticated adversary uses MS-NRPC to connect to a domain controller for obtaining Domain Admin access to exploit a vulnerability.

Secura, whose researcher discovered the vulnerability, released a [blog](#) that outlines the technical details of the flaw. The researcher stated that “the vulnerability stems from a flaw in a cryptographic authentication scheme used by the Netlogon Remote Protocol, which among other things, can be used to update computer passwords. This flaw allows attackers to impersonate any computer, including the domain controller itself, and execute remote procedure calls on their behalf.”

On September 14, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) acknowledged the ZeroLogon vulnerability's severity and [issued a security advisory](#) encouraging users and administrators to apply the necessary updates.

Several proof-of-concept (PoC) codes have been released in [Github](#), giving attackers full access to companies' domain controllers (DCs). Also, the [new Mimikatz release](#) detects and exploits the ZeroLogon vulnerability.

Furthermore, [Microsoft released another advisory](#) that details how to manage the changes in the Netlogon secure channel connections associated with CVE-2020-1472 after the patch installation.

## Detecting the ZeroLogon vulnerability

To detect the abuse of the ZeroLogon vulnerability, look for the event ID 4742. To be specific, hunt for ANONYMOUS LOGON users, and SID in the event ID 4742 with the Password Last Set field changed.

Event 4742, Microsoft Windows security auditing.

General Details

A computer account was changed.

Subject:

Security ID:	ANONYMOUS LOGON
Account Name:	ANONYMOUS LOGON
Account Domain:	NT AUTHORITY
Logon ID:	0x3E6

Computer Account That Was Changed:

Security ID:	MOON\OVERLORDS
Account Name:	OVERLORDS
Account Domain:	MOON

Changed Attributes:

SAM Account Name:	-
Display Name:	-
User Principal Name:	-
Home Directory:	-
Home Drive:	-
Script Path:	-
Profile Path:	-
User Workstations:	-
Password Last Set:	9/17/2020 11:28:46 PM
Account Expires:	-

Log Name: Security

Source: Microsoft Windows security

Event ID: 4742

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 9/17/2020 11:28:46 PM

Task Category: Computer Account Management

Keywords: Audit Success

Computer: Overlord.moon.local

You can also look for account change-related activity of all domain controllers in the Active Directory.

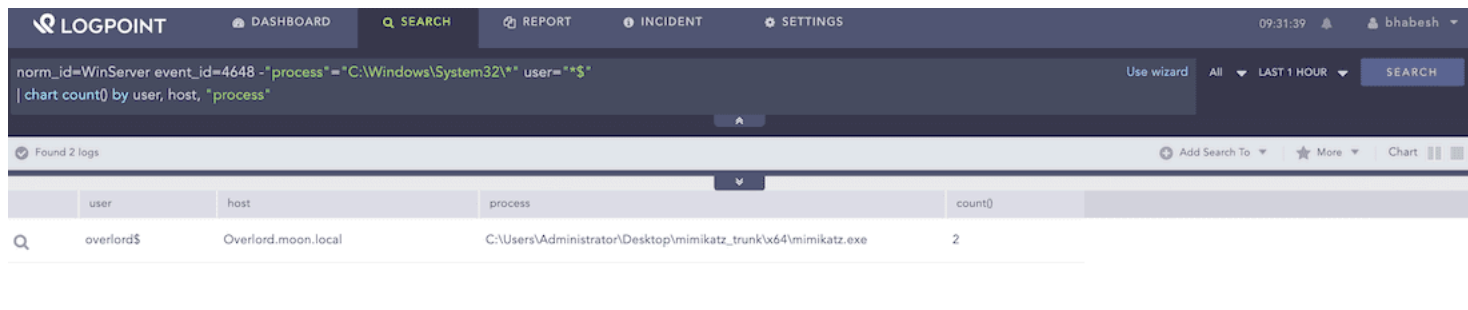
```
norm_id=WinServer label=Computer label=Account label=Change computer=* user="ANONYMOUS LOGON" user_id="S-1-5-7" password_last_set_ts=*
```

In August's update, Microsoft added five new event IDs to notify vulnerable Netlogon connections. For example, the event ID 5829 is generated when a vulnerable Netlogon secure channel connection is allowed during an initial deployment phase.

```
norm_id=WinServer event_id=5829
```

Furthermore, admins can monitor event IDs 5827 and 5828, triggered when vulnerable Netlogon connections are denied, and event IDs 5830 and 5831, triggered when vulnerable Netlogon connections are allowed by the patched domain controllers via Group Policy. However, after the patch installation, domain controllers may experience a sudden increase in the number of these events in the System log.

To detect Mimikatz trying to exploit ZeroLogon, look for the event ID 4648 (Logins using explicit credentials) with suspicious processes.



The screenshot shows the Logpoint SIEM interface. At the top, there's a navigation bar with 'LOGPOINT' logo and tabs for 'DASHBOARD', 'SEARCH', 'REPORT', 'INCIDENT', and 'SETTINGS'. The 'SEARCH' tab is active. Below the navigation bar, a search query is entered: `norm_id=WinServer event_id=4648 -"process"="C:\Windows\System32\*" user="*$"`. Below the query, there's a table with columns: user, host, process, and count(). The table contains one row: `overlord$`, `Overlord.moon.local`, `C:\Users\Administrator\Desktop\mimikatz_trunk\w64\mimikatz.exe`, and `2`.

user	host	process	count()
overlord\$	Overlord.moon.local	C:\Users\Administrator\Desktop\mimikatz_trunk\w64\mimikatz.exe	2

Finally, unpatched systems are an attractive target for malicious actors. We advise that system administrators install the patch from [August's Patch Tuesday](#) for all domain controllers to avoid compromise. As of now, Mimikatz is armed with Zerologon. Given the circumstance, it is crucial to monitor its activity in your environment.

## Discover More About Logpoint

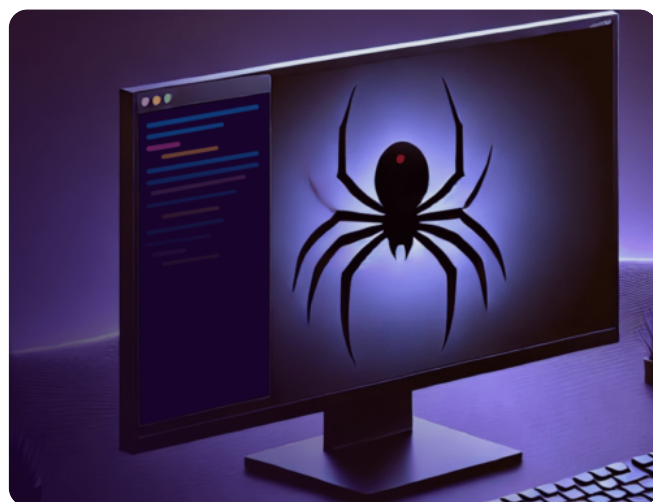
[Book a demo](#)[Customer cases](#)[Customer reviews](#)

## Related Posts



### Uncover more resources with Logpoint's latest release

October 30th, 2024



### Latrodectus: The Wrath of Black Widow

October 22nd, 2024



Detect. Manage. Respond.

Products

- SIEM
- Automation
- Case Management
- Behavior Analytics
- Cyber Defense Platform
- Pricing
- Sizing Calculator

Why Logpoint?

- Product Recognition
- Customer Cases
- EAL3+ Certificate
- Newsletter



Company

- About us
- Management
- Careers at Logpoint
- Media Room
- Logpoint in the media
- Blog & Webinars

Support

- Cyber Library
- Service Desk
- Documentation
- Community
- Contact
- Status

Contact

-  [info@logpoint.com](mailto:info@logpoint.com)
-  +45 7060 6100
- 