WDigest Clear-Text Passwords: Stealing More than a Hash

blog.netwrix.com/2022/10/11/wdigest-clear-text-passwords-stealing-more-than-a-hash

Kevin Joyce

What is WDigest?

Digest Authentication is a challenge/response protocol that was primarily used in Windows Server 2003 for LDAP and web-based authentication. It utilizes Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges to authenticate.

At a high level, a client requests access to something, the authenticating server challenges the client, and the client responds to the challenge by encrypting its response with a key derived from the password. The encrypted response is compared to a stored response on the authenticating server to determine if the user has the correct password. Microsoft provides a much more in-depth explanation of WDigest.

What security risk does WDigest introduce?

WDigest stores clear-text passwords in memory. Therefore, if an adversary who has access to an endpoint can use a tool like Mimikatz to get not just the hashes stored in memory, but the clear-text passwords as well. As a result, they will not be limited to attacks like Pass-the-Hash; they'd also be able to log on to Exchange, internal web sites, and other resources that require entering a user ID and password.

For example, suppose the user "TestA" used remote desktop to log on to a machine, leaving their password in memory. The screenshot below illustrates what an attacker would see when dumping credentials from that machine's memory using Mimikatz. As you can see, they get both the NTLM password hash for the account and the clear-text password "Password123" as well.

What can be done to mitigate this risk?

Fortunately, Microsoft released a security update (KB2871997) that allows organizations to configure a registry setting to prevent WDigest from storing clear-text passwords in memory. However, doing so will leave WDigest unable to function, so Microsoft recommends first seeing whether Digest authentication is being used in your environment. Check the event logs on your servers for event ID 4624 and check your domain controller logs for event ID 4776 to see if any users have logged in with 'Authentication Package: WDigest'. Once you're sure that there are no such events, you can make the registry change without impacting your environment.

Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012

For Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012, install update KB2871997 and then set the following registry key to 0:

The easiest way to do this is through Group Policy, but the following script will also work:

```
reg add
HKLMSYSTEMCurrentControlSetControlSecurityProvidersWDigest /v
UseLogonCredential /t REG_DWORD /d 0
```

Later Versions of Windows and Windows Server

Later versions of Windows and Windows Server do not require the security update, and the registry value is set to 0 by default. However, you should verify that the value hasn't been manually changed by using the following script:

```
reg query
HKLMSYSTEMCurrentControlSetControlSecurityProvidersWDigest /v
UseLogonCredential
```

Results

Once this registry value has been set to 0, an attacker dumping credentials out of memory wouldn't get the clear-text password; instead, they would see this:

Reference Chart

Here's a chart to help you determine if you need to take action on your endpoints:

Quick Recap

WDigest stores clear-text credentials in memory, where an adversary could steal them. Microsoft's security update KB2871997 addresses the issue on older versions of Windows and Windows Server by enabling you to set a registry value, and newer versions have the proper value by default.

Checking this registry setting on all of your Windows endpoints should be a priority, as credential theft can lead to the loss of sensitive information. One way to do this is to run command-line queries against all your hosts; a quicker option is to automate the process with an auditing solution that provides the results in an easy-to-consume report.

How can Netwrix help?

Netwrix StealthAUDIT can help you enhance the security of your Windows infrastructure and minimize the risk of a data breach. It empowers you to:

- Identify vulnerabilities that can be used by attackers to compromise Windows systems and get to your data.
- Enforce security and operational policies through baseline configuration analysis.
- Audit and govern privileged accounts.
- Prove compliance more easily with prebuilt reports and complete system transparency.

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.