Microsoft Security Advisory: Update to improve credentials protection and management: May 13, 2014

INTRODUCTION

Microsoft has released a Microsoft security advisory about this problem for IT professionals. The security advisory contains additional security-related information. To view the security advisory, go to the following Microsoft website:

https://technet.microsoft.com/security/advisory/2871997Important In addition to update 2871997, there have been multiple other updates that contribute to improving credential protection. Please read this article carefully to understand the entire set of updates that are available.

Update FAQ

Does this update contain any additional security-related changes to functionality?
In addition to the changes that are listed for the vulnerabilities described in this bulletin, this update includes defense-in-depth updates to help improve credential protection and domain authentication controls to reduce credential theft. For more information see Microsoft Security Advisory 2871997.

More Information

This update introduces a TokenLeakDetectDelaySecs registry setting

ImportantThis section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:

322756How to back up and restore the registry in Windows
After you install this security update, the default setting for non-protected users on Windows 7 and Windows 8 is to not force clear leaked logon session credentials. To override this default you can add the following registry dword, and set it to a recommended value of 30 seconds.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\TokenLeakDetectDelaySecs

This will trigger the clearing of any credentials of logged off users after 30 seconds, regardless if there is a still a reference to it. This is the same as the default behavior for Windows 8.1 and Windows 10.

Default behavior after applying security update 3126593 (MS16-014)

After you install security update 3126593, the default is to force clear credentials for all users. If you wish to revert to previous legacy behavior, set the TokenLeakDetectDelaySecs entry to 0. This disables the clearing of credentials of logged off non-protected users as long as a reference remains.

Revisions

On October 14, 2014, Microsoft released the following updates to add a Restricted Admin mode for Remote Desktop Connection and Remote Desktop Protocol:

2984972 for supported editions of Windows 7 and Windows Server 2008 R2

2984976 for supported editions of Windows 7 and Windows Server 2008 R2 that have update 2592687 (Remote Desktop Protocol 8.0 update) installed. Customers who install update 2984976 must also install update 2984972.

2984981 for supported editions of Windows 7 and Windows Server 2008 R2 that have update 2830477 (Remote Desktop Connection 8.1 client update) installed. Customers who install update 2984981 must also install update 2984972.

2973501 for supported editions of Windows 8, Windows Server 2012, and Windows RT.
Note Supported editions of Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1 already include this feature and do not require this update.

On September 9, 2014, Microsoft released the following:

2982378 Microsoft Security Advisory: Update to improve credentials protection and management for Windows 7 and Windows Server 2008 R2: September 9, 2014 On July 8, 2014, Microsoft released the following:

2973351 Microsoft Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed: July 8, 2014

2975625 Microsoft Security Advisory: Registry update to improve credentials protection and management for Windows systems that do not have the 2919355 update installed: July 8, 2014 This update provides configurable registry settings for managing the Restricted Admin mode for Credential Security Support Provider (CredSSP).

Note The update changes default Restricted Admin mode functionality in Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1. For more information, see the FAQ section of the advisory. The following files are available for download from the Microsoft Download Center.

Note Use the following table to determine which updates are appropriate for your system.

Security update KB number	Operating system
2973351	Windows 8.1 and Windows Server 2012 R2 systems that have update 2919355 installed
2975625	Windows 8.1 and Windows Server 2012 R2 systems that do not have update 2919355 installed
2973501	Windows 8, Windows Server 2012, and Windows RT

2871997	Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012
2973351	Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012
2982378	Windows 7 and Windows Server 2008 R2
2984972	Windows 7 and Windows Server 2008 R2
2984976	Windows 7 and Windows Server 2008 R2 that have update 2592687 installed. 2984972 must also be installed.
2984981	Windows 7 and Windows Server 2008 R2 that have update 2830477 installed. 2984972 must also be installed

WDigest settings

After you install this security update, you can control how installed WDigest credentials can be saved by using a registry setting. To prevent WDigest credentials from being stored in memory, a Group Policy setting can be applied to the **UseLogonCredential** registry entry under the following subkey:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest

- If the UseLogonCredential value is set to **0**, WDigest will not store credentials in memory.
- If the UseLogonCredential value is set to **1**, WDigest will store credentials in memory.

After you install this security update, the default setting for this value is **1** in Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012. You can use the "easy fix" solution in this article to change this setting to **0**. This will disable WDigest passwords from being stored in memory.

Note By default in Windows 8.1 and Windows Server 2012 R2 and **later versions**, caching of credentials in memory for WDigest is disabled (the **UseLogonCredential** value defaults to 0 when the registry entry is not present).

The observed change in behavior when the **UseLogonCredential** value is set to **0** is that you may notice that credentials are required more frequently when you use WDigest.

Here's an easy fix

This easy fix solution changes the **UseLogonCredential** registry key to disable WDigest passwords from being stored in memory. After you install security update 2871997, and then you apply this easy fix solution to systems that are running Windows 7, Windows Server 2008 R2, Windows 8, or Windows Server 2012, you should no longer have Basic (clear text) credentials stored in memory.

Note You must have security update 2871997 installed before you can use this easy fix solution.

To enable this easy fix solution, click the **Download** button. In the **File Download** dialog box, click **Run** or **Open**, and then follow the steps in the easy fix wizard.

- This wizard may be in English only. However, the automatic fix also works for other language versions of Windows.

- If you're not on the computer that has the problem, save the easy fix solution to a flash drive or a CD, and then run it on the computer that has the problem.

Disable WDigest passwords from being stored in memory

Microsoft Download Center

FILE INFORMATION

The English (United States) version of this software update installs files that have the attributes that are listed in the following tables. The dates and times for these files are listed in Coordinated Universal Time (UTC). The dates and times for these files on your local computer are displayed in your local time and with your current daylight saving time (DST) bias. Additionally, the dates and times may change when you perform certain operations on the files.

Windows 7 and Windows Server 2008 R2 file information

Windows 8 and Windows Server 2012 file information

File hash information

Need more help?

How can we help you?

Want more options?

Discover Community

Explore subscription benefits, browse training courses, learn how to secure your device, and more.

Microsoft 365 subscription benefits | Microsoft 365 training | Microsoft security | Accessibility center

Was this information helpful? Yes No