Microsoft Security Advisory 4053440

By BetaFred

Archived: 2026-04-02 10:35:52 UTC

Securely opening Microsoft Office documents that contain Dynamic Data Exchange (DDE) fields

Published: November 8, 2017 | Updated: January 9, 2018

Version: 3.0

Executive Summary

Microsoft is releasing this security advisory to provide information regarding security settings for Microsoft Office applications. This advisory provides guidance on what users can do to ensure that these applications are properly secured when processing Dynamic Data Exchange (DDE) fields.

About Dynamic Data Exchange

Microsoft Office provides several methods for transferring data between applications. The DDE protocol is a set of messages and guidelines. It sends messages between applications that share data, and uses shared memory to exchange data between applications. Applications can use the DDE protocol for one-time data transfers and for continuous exchanges in which applications send updates to one another as new data becomes available.

Scenario

In an email attack scenario, an attacker could leverage the DDE protocol by sending a specially crafted file to the user and then convincing the user to open the file, typically by way of an enticement in an email. The attacker would have to convince the user to disable Protected Mode and click through one or more additional prompts. As email attachments are a primary method an attacker could use to spread malware, Microsoft strongly recommends that customers exercise caution when opening suspicious file attachments.

DDE Feature Control Keys

Microsoft Office provides several feature control keys that are stored in the registry and are responsible for modifying product functionality, improving support for industry standards, and improving security. Microsoft has documented these feature control keys and recommends enabling specific feature control keys for security reasons. See the following:

- Office 2016: Secure and control access to Office
- Office 2013: Secure Office 2013

Microsoft strongly encourages all users of Microsoft Office to review the security-related feature control keys and to enable them. Setting the registry keys described in the following sections disables automatic update of data from linked fields.

Update On December 12, 2017, Microsoft released an update for all supported editions of Microsoft Word that allows users to set the functionality of the DDE protocol based on their environment. For more information and to download the update, see ADV170021.

Update On January 9, 2018, Microsoft released an update for all supported editions of Microsoft Excel that allows users to set the functionality of the DDE protocol based on their environment. For more information and to download the update, see ADV170021.

Mitigating DDE Attack Scenarios

Users who wish to take immediate action can protect themselves by manually creating and setting registry entries for Microsoft Office. Use the following instructions to set the registry keys based on the Office applications installed on your system.

Warning: If you use Registry Editor incorrectly, you could cause serious problems that could require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

Microsoft recommends that you back up your Registry before making any changes to registry entries.

Microsoft Excel

Excel depends on the DDE feature to launch documents.

To prevent automatic update of links from Excel (including DDE, OLE, and external cell or defined name references), refer to the following table for the registry key version string to set for each version:

Office Version	Registry Key <version> string
Office 2007	12.0
Office 2010	14.0
Office 2013	15.0
Office 2016	16.0

- To disable the DDE feature via the user interface:
  Set File->Options->Trust Center->Trust Center Settings…->External Content->Security settings for Workbook Links = Disable automatic update of Workbook Links.
- To disable the DDE feature via the Registry Editor:

```
 [HKEY_CURRENT_USER\Software\Microsoft\Office\</version><version>\Excel\Security]
WorkbookLinkWarnings(DWORD) = 2
```

Impact of mitigation: Disabling this feature could prevent Excel spreadsheets from updating dynamically if disabled in the registry. Data might not be completely up-to-date because it is no longer being updated automatically via live feed. To update the worksheet, the user must start the feed manually. In addition, the user will not receive prompts to remind them to manually update the worksheet.

Microsoft Outlook

Refer to the following table for the registry key version string to set for each Office version:

Office Version	Registry Key </version> string
Office 2010	14.0
Office 2013	15.0
Office 2016	16.0

- For Office 2010 and later versions, to disable the DDE feature via the Registry Editor:

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\</version><version>\Word\Options\WordMail]
 DontUpdateLinks(DWORD)=1
```

- For Office 2007, to disable the DDE feature via the Registry Editor:

```
 [HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\vpref]
fNoCalclinksOnopen_90_1(DWORD)=1
```

Impact of mitigation: Setting this registry key will disable automatic update for DDE field and OLE links. Users can still enable the update by right-clicking on the field and clicking “Update Field”.

Microsoft Publisher

A Word document using the DDE protocol that is imbedded within a Publisher document could be a possible attack vector. You can help prevent this attack vector by applying the Word registry key modification. See the following section for the Word registry key values.

Microsoft Word

See ADV170021 for an update for Microsoft Word that allows users to set the functionality of the DDE protocol based on their environment.

Refer to the following table for the registry key version string to set for each Office version:

Office Version	Registry Key </version> string
Office 2010	14.0
Office 2013	15.0
Office 2016	16.0

- For Office 2010 and later versions, to disable the DDE feature via the Registry Editor:

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\</version><version>\Word\Options]
DontUpdateLinks(DWORD)=1
```

- For Office 2007, to disable the DDE feature via the Registry Editor:

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\vpref]
fNoCalclinksOnopen_90_1(DWORD)=1
```

Impact of mitigation: Setting this registry key will disable automatic update for DDE field and OLE links. Users can still enable the update by right-clicking on the field and clicking “Update Field”.

Windows 10 Fall Creators Update (version 1709)

Users of the Windows 10 Fall Creators Update can leverage Windows Defender Exploit Guard to block DDE-based malware with Attack surface reduction (ASR) rules.

ASR is a component within Windows Defender Exploit Guard that provides enterprises with a set of built-in intelligence that can block the underlying behaviors used by malicious documents to execute attacks without hindering product operation. By blocking malicious behaviors independent of what the threat or exploit is, ASR can protect enterprises from never-before-seen zero-day attacks like these recently discovered vulnerabilities: CVE-2017-8759, CVE-2017-11292, and CVE-2017-11826.

For Office apps, ASR can:

- Block Office apps from creating executable content
- Block Office apps from launching child process
- Block Office apps from injecting into process
- Block Win32 imports from macro code in Office
- Block obfuscated macro code

Emerging exploits like DDEDownloader use the Dynamic Data Exchange (DDE) popup in Office documents to run a PowerShell downloader; however, in doing so, they launch a child process that the corresponding child process rule blocks.

Windows Defender Exploit Guard can be used with Windows Defender Advanced Threat Protection (ATP) to investigate and respond to enterprise-level security risks and issues. To learn more about Windows Defender

Exploit Guard and Windows Defender ATP, see:

- Windows Defender Exploit Guard
- Windows Defender Advanced Threat Protection
- Enroll in a free trial for Windows Defender ATP
- Windows Defender Exploit Guard: Reduce the attack surface against next-generation malware

Microsoft is researching this issue further and will post more information in this article when the information becomes available.

Additional Suggested Actions

- **Protect your PC**
  We continue to encourage customers to follow our Protect Your Computer guidance of enabling a firewall, getting software updates, and installing antivirus software. For more information, see Microsoft Safety & Security Center.
- **Keep Microsoft Software Updated**
  Users running Microsoft software should apply the latest Microsoft security updates to help make sure that their computers are as protected as possible. If you are not sure whether your software is up to date, visit Microsoft Update, scan your computer for available updates, and install any high-priority updates that are offered to you. If you have automatic updating enabled and configured to provide updates for Microsoft products, the updates are delivered to you when they are released, but you should verify that they are installed.

Other Information

Disclaimer

The information provided in this advisory is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

- V1.0 (November 8, 2017): Advisory published.
- V1.1 (November 30, 2017): Updated the Windows 10 Fall Creators Update section with more information about the Attack surface reduction (ASR) rules. This is an informational change only.
- V2.0 (December 12, 2017): Microsoft has released an update for all supported editions of Microsoft Word that allows users to set the functionality of the DDE protocol based on their environment. For more information and to download the update, see ADV170021.

- V3.0 (January 9, 2018): Microsoft has released an update for all supported editions of Microsoft Excel that allows users to set the functionality of the DDE protocol based on their environment. For more information and to download the update, see ADV170021.
