# Microsoft Disables DDE Feature in Word to Prevent Further Malware Attacks

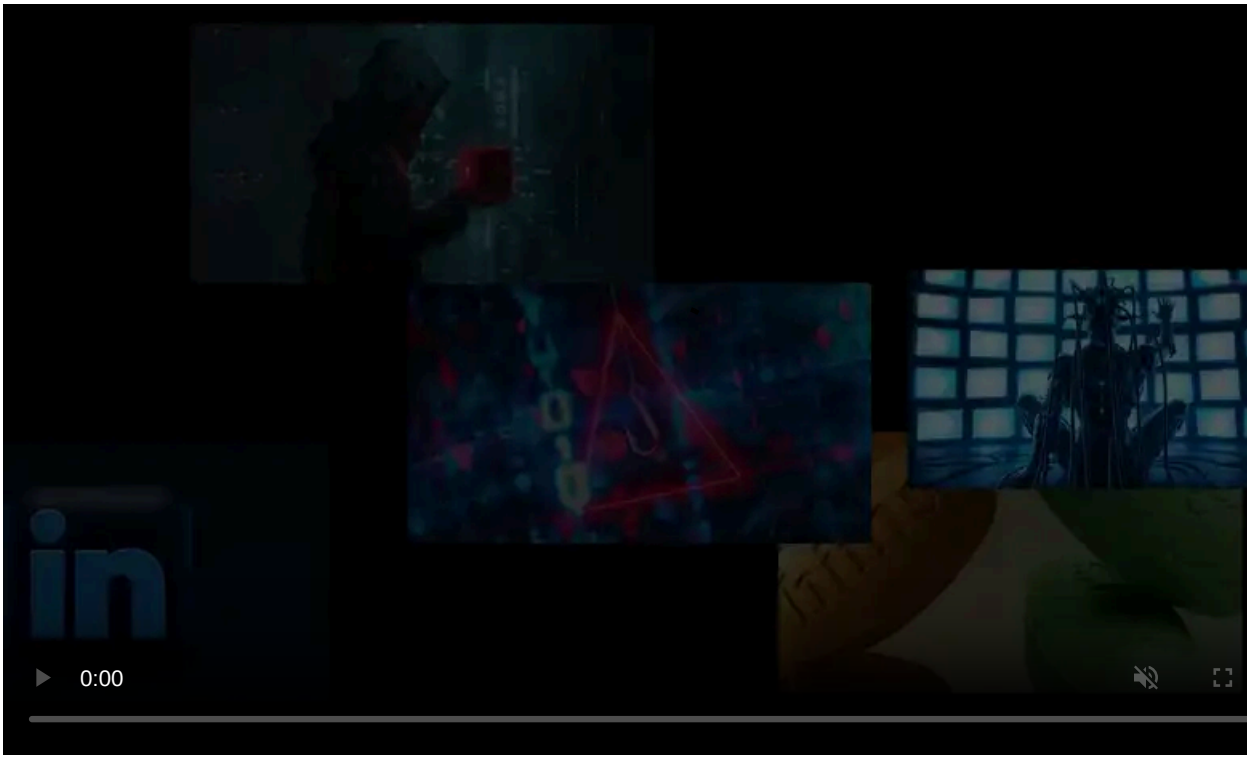
By Catalin Cimpanu

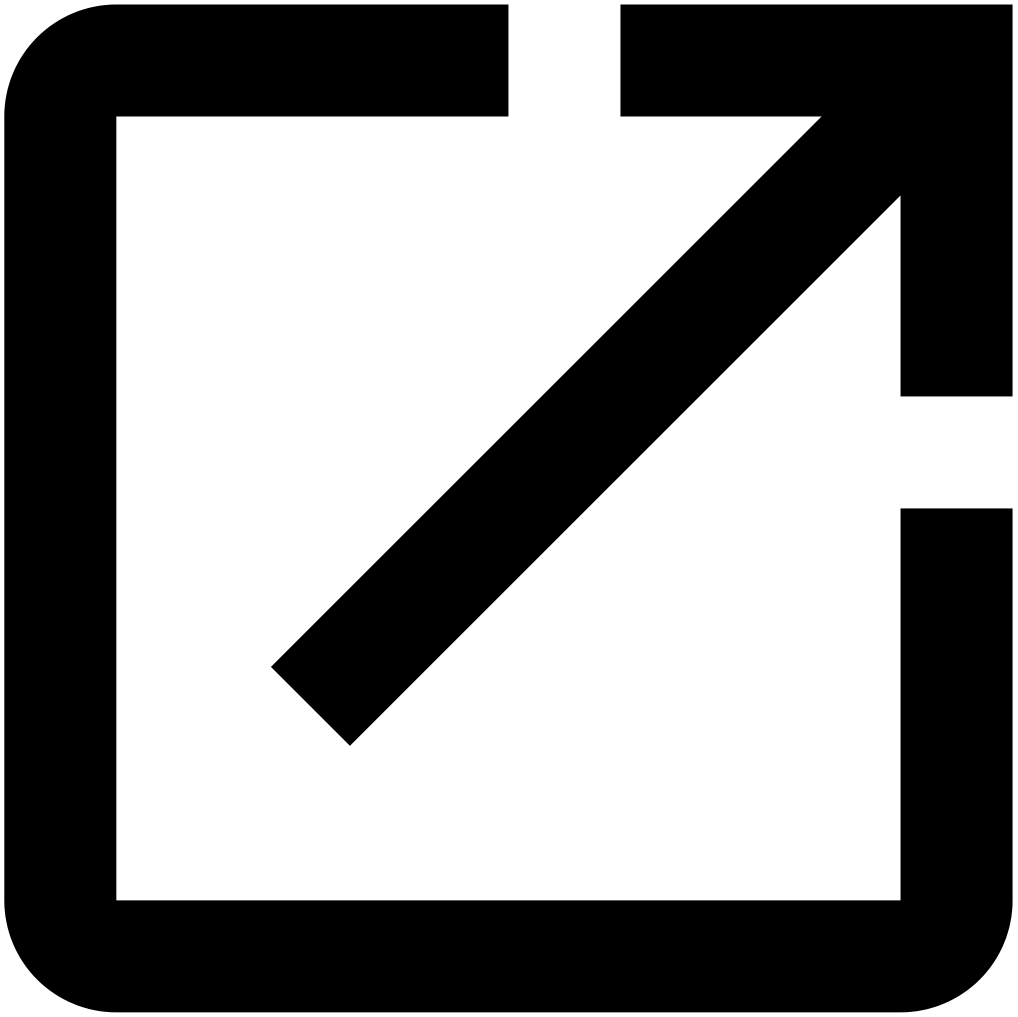
Published: 2017-12-15 · Archived: 2026-04-05 18:45:47 UTC

As part of the December 2017 Patch Tuesday, Microsoft has shipped an Office update that disables the DDE feature in Word applications, after several malware campaigns have abused this feature to install malware.

DDE stands for Dynamic Data Exchange, and this is an Office feature that allows an Office application to load data from other Office applications. For example, a Word file can update a table by pulling data from an Excel file every time the Word file is opened.

DDE is an old feature, which Microsoft has superseded via the newer Object Linking and Embedding (OLE) toolkit, but DDE is still supported by Office applications.


0:00



## DDE feature abused to install malware

In October 2017, security researchers from SensePost published a tutorial on how the DDE feature could be weaponized and abused to distribute malware.

Even if DDE has been abused to distribute malware in the '90s, the new methods explained in the SensePost tutorial were quickly adopted by malware distributors, first by FIN7, a group of hackers specialized in hitting financial organizations, and then by distributors of mundane malware.

At the time, Microsoft did not consider DDE a vulnerability in the Office suite but said it was just another legitimate feature abused to distribute malware.

The reason why Microsoft did not consider DDE attacks to be security issues is that Office shows warnings before opening the files. This is just another case where malware authors have found a creative way of abusing a legitimate feature, like with OLE and macros, for which Microsoft also warns users before running.

## December 2017 Patch Tuesday disables DDE in Word

As new campaigns leveraging the DDE technique started to become more widespread, Microsoft's security team slowly began to change its mind.

The first sign was when Microsoft put out Security Advisory 4053440 in mid-October, which contained details about how users could disable the DDE feature in Office applications that support it, such as Word, Outlook, and Excel.

This past Tuesday, Microsoft took a radical step to disable DDE inside Word altogether. This has been done by Office Defense in Depth Update ADV170021.

This update adds a new Windows registry key that controls the DDE feature's status for the Word app. The default value disables DDE. Here are registry key's values, if users need to re-enable DDE in Word.

1. In the Registry Editor navigate to \HKEY_CURRENT_USER\Software\Microsoft\Office\version\Word\Security AllowDDE(DWORD)
2. Set the DWORD value based on your requirements as follows:

**AllowDDE(DWORD) = 0**: To disable DDE. This is the default setting after you install the update.
**AllowDDE(DWORD) = 1**: To allow DDE requests to an already running program, but prevent DDE requests that require another executable program to be launched.
**AllowDDE(DWORD) = 2**: To fully allow DDE requests.

Microsoft has paid close attention to DDE's recent abuse so much so that ADV170021 also included updates for Word 2003 and 2007, two versions it officially stopped supporting.

The company is aware that many users and enterprises still deploy these two versions and has delivered an out-of-band emergency update to protect customers from further abuse.

Microsoft will continue to support DDE inside Excel and Outlook, where this feature will remain enabled by default. The company advises users to read Security Advisory 4053440, where it details methods to disable DDE support via GUI options or Windows registry modifications.

---

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/