Sandworm Windows zero-day vulnerability being actively exploited in targeted attacks

Published: 2014-10-14 · Archived: 2026-04-05 18:54:44 UTC

A critical new vulnerability in the Windows operating system is reportedly being exploited in a limited number of attacks against targets in the US and Europe. The Microsoft Windows OLE Package Manager Remote Code Execution Vulnerability (CVE-2014-4114) allows attackers to embed Object Linking and Embedding (OLE) files from external locations. The vulnerability can be exploited to download and install malware on to the target's computer. The vulnerability appears to have been used by a cyberespionage group known as Sandworm to deliver Backdoor.Lancafdo.A (also known as the Black Energy back door) to targeted organizations.

The vulnerability affects all versions of Windows from Windows Vista Service Pack 2 right up to to Windows 8.1 and Windows Server versions 2008 and 2012. It relates to how Windows handles OLE, a Microsoft technology that allows rich data from one document to be embedded in another or a link to a document to be embedded in another. OLE is generally used for embedding locally stored content, but this vulnerability enables the unprompted download and execution of external files.

Active exploitation underway

The vulnerability was disclosed by iSIGHT Partners, which said that the vulnerability had already been exploited in a small number of cyberespionage attacks against NATO, several unnamed Ukrainian government organizations, a number of Western European governmental organization, companies operating in the energy sector, European telecoms firms, and a US academic organization. According to our telemetry, attacks using this payload have been underway since August. iSIGHT has attributed these attacks to an advanced persistent threat (APT) group it has named Sandworm.

Attacks to date have seen targeted individuals receive a spear-phishing email containing a malicious PowerPoint file attachment, which is detected by Symantec as Trojan.Mdropper. The PowerPoint file contains two embedded OLE documents containing URLs. If the targeted user opens the PowerPoint file, these URLs are contacted and two files are downloaded, one .exe and one .inf, which will install malware on the computer. Symantec detects this malware payload as Backdoor.Lancafdo.A.

Once installed on the target's computer, this back door allows attackers to download and install other malware. The malware may also download updates for itself, including an information-stealing component.

While the current exploits are using PowerPoint files, given the nature of the vulnerability, we may eventually see this exploit crop up in different Office file types such as Word documents or Excel spreadsheets.

Symantec regards this vulnerability as critical, since it allows attackers to remotely run code on the target's computer. While it has been exploited on a limited basis in the wild, other groups are likely to attempt to take advantage of it now that its existence has been publicized.

Advice for businesses and consumers

Symantec advises all affected Windows users to take the following actions.

- Immediately apply security patches once available from Microsoft
- Ensure that your security software is up-to-date
- Exercise caution when opening email attachments, particularly from unknown sources

Symantec protection

Symantec customers are protected against the malware being used in attacks exploiting this vulnerability with the following detections.

Antivirus

- Backdoor.Lancafdo
- Backdoor.Lancafdo.A
- Trojan.Mdropper

Intrusion Prevention

- Attack: Malicious File Download

Update–October 15, 2014:

Microsoft has now issued a security bulletin which provides a patch for the vulnerability. Symantec recommends

that all users apply the patch published in Microsoft Security Bulletin MS14-060.
