Security Response

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

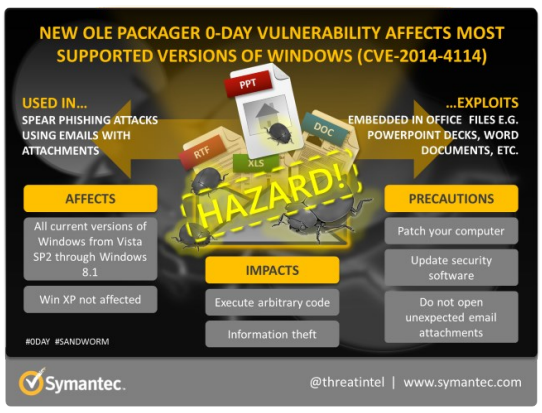
Critical new Windows zero-day has reportedly been used in a limited number of targeted cyberespionage attacks to deliver a back door on to the victim's computer.

Created: 14 Oct 2014 15:38:06 GMT • Updated: 18 Nov 2014 20:55:35 GMT • Translations available: 日本語, 한국어, Português

Symantec Security Response SYMANTEC EMPLOYEE

+3 3 Votes

Symantec. | Official Blog



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 organizations, 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. Symantec customers that use the Symantec.Cloud service are protected from spam messages used to deliver malware.

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.

Blog Entry Filed Under:
Security, Security Response, Endpoint Protection (AntiVirus), Backdoor.Lancafdo, Cyberespionage, Microsoft, OLE Package Manager, Remote Code Execution, Sandworm, Trojan.Mdropper, Windows, zero-day vulnerability

Upcoming Events

Philadelphia Security & Compliance User Group Meeting - January 28, 2015
28 Jan, 2015 - 9:00 EST

Symantec Control Compliance Suite 11.0: Administration
02 Feb, 2015 - 11:00 EST

End of Support Should Not End Your Business: Planning for Windows Server 2003 End of Life
19 Feb, 2015 - 10:00 PST

Symantec Control Compliance Suite (CCS) 11.0 Administration
02 Mar, 2015 - 9:00 CST

Links

- Technical Support
- Symantec Training
- Symantec.com
- Purchase Endpoint Protection Small Business Edition
- Purchase SSL Certificates
- Website Security Solutions Knowledge Base

About Security Response Blog

Our security research centers around the world provide unparalleled analysis of and protection from malware, security risks, vulnerabilities, and spam.

Recent Blog Posts

- LinkedIn Alert: Scammers use security update to phish for credentials • Satnam Narang • 14 Jan 2015 15:59:28 GMT
- Japanese one-click fraud evolves to lock smartphone browsers • Joji Hamada • 14 Jan 2015 03:06:06 GMT
- New Carberp variant heads down under • Roberto Sponchioni • 14 Jan 2015 11:24:01 GMT
- Microsoft Patch Tuesday – January 2015 • PraveenSingh • 14 Jan 2015 00:46:14 GMT
- Mobile spyware makers are on shaky ground as the law begins to catch up with them • Laura O'Brien • 18 Dec 2014 14:51:49 GMT

Filter by:

Author

English

Recently on Twitter

- France sees 19K websites targeted since January 7 terror attacks http://t.co/VBNRzc5qY6 #France 17 Jan 2015
- Oops! Security and military experts connect to Wi-Fi honeypot at Swedish conference http://t.co/7k0v5Li8u #Sweden 17 Jan 2015
- Rise of "hacker-for-hire" poses problems, lowers entry barrier to online crime http://t.co/CQQcSCrywb #cybercrime 16 Jan 2015
- What is your #password? WATCH: Jimmy Kimmel (@jimmykimmel) show how carefree we are about digital security https://t.co/VmWZEu55VE 16 Jan 2015
- Fake news from @NYPost and @UPI after Twitter accounts briefly hacked http://t.co/wzxo4slytM 16 Jan 2015

Blog Tags

Endpoint Protection (AntiVirus) Spam Online Fraud phishing Malicious Code Messaging Gateway Message Filter Symantec Protection Suites (SPS) Mail Security for Exchange/Domino Vulnerabilities & Exploits Email Security.cloud Encryption Desktop Email Encryption Symantec Endpoint Encryption - Device Control Security Risks Emerging Threats Android Microsoft Patch Tuesday Evolution of Security Trojan.Zbot facebook Mobile & Wireless W32.Stuxnet scam Malware

Security Response Blog Archive