Microsoft Zero Day Traced to Russian ‘Sandworm’ Hackers

By Phil Muncaster

Published: 2014-10-14 · Archived: 2026-04-05 13:20:47 UTC

Threat intelligence firm iSight Partners has announced the discovery of a new remote code execution zero day vulnerability affecting all supported versions of Microsoft Windows, Server 2008 and 2012, and linked to a Russian espionage group known as "Sandworm."

The vulnerability, CVE-2014-4114, was discovered by iSight at the beginning of September in spear-phishing attacks from “Sandworm Team” using a weaponized PowerPoint attachment, the firm said in a blog post.

It will be patched in today’s monthly security update from Microsoft.

The flaw exists in the in the “OLE package manager” in Windows and Microsoft Server, allowing an attacker to remotely execute arbitrary code if they can convince a victim to open a specially crafted file via social engineering techniques.

“The vulnerability exists because Windows allows the OLE packager (packager .dll) to download and execute INF files,” the firm explained.

“In the case of the observed exploit, specifically when handling Microsoft PowerPoint files, the packagers allows a Package OLE object to reference arbitrary external files, such as INF files, from untrusted sources. This will cause the referenced files to be downloaded in the case of INF files, to be executed with specific commands.”

The threat intelligence firm said it has been working with Microsoft to monitor the use of the vulnerability and work on a patch, and added that it appears to have been used only by the Sandworm group.

The group itself has been referenced in the past by ESET and F-Secure (which named it “Quedagh”) in relation to BlackEnergy attacks on various entities in Eastern Europe and elsewhere.

It has likely been in operation since 2009, and has attacked NATO members in 2013, attendees of security forum Globsec the following year, a Polish energy firm and a French telecoms firm, said iSight.

Many of the lures used in the spear-phishing emails related to the Ukrainian conflict and “broader geopolitical issues related to Russia,” with Ukrainian government targets also singled out.

The “Sandworm” moniker was so chosen due to references to sci-fi novel series Dune in command and control URLs and various malware samples, iSight said.

Ollie Whitehouse, technical director at information assurance firm NCC Group, described CVE-2014-4114 as "pervasive and trivial to exploit."

This event should remind organisations of the need to have robust patch management policies and procedures in place," he added.

"The ease with which organisations can be targeted in such a way is more of a concern. This is why regular practical training and simulation for staff to recognise these sorts of attacks and to understand the organisation’s susceptibility is incredibly important.”
