

Adobe PDF exploit infects 'many thousands,' says researcher

Adobe credits New Zealand-based Security-Assessment.com, among others, for reporting the bugs

BY GREGG KEIZER | FRAMINGHAM | TUESDAY, 12 FEBRUARY, 2008

EMAIL PRINT

Attackers have been exploiting one of the recently-revealed vulnerabilities in Adobe Reader for at least three weeks, say security researchers, with one estimating the infection count at "many thousands" so far.

On Tuesday last week, Adobe Systems acknowledged that its popular PDF viewer sported several flaws, and patched them that same day. However, it has yet to spell out the exact number or nature of the bugs.

But one of those vulnerabilities has been actively exploited since at least Jan. 20, said researchers at the SANS Institute's Internet Storm Center (ISC) and VeriSign's iDefense unit. According to Raul Siles, an analyst with ISC, a malicious PDF (Portable Document Format) file has been spreading a Trojan horse from a server based in the Netherlands. The first evidence of the attack, said Siles, came in a Jan. 20 message on an Italian message forum from a user who noted that three of his PCs had been infected, and the attack was traced back to the Dutch IP address.

Siles quoted email he received from iDefense researchers, who said that the malware, a variation of the "Zonebac" Trojan horse, disables a slew of antivirus programs and modifies search results and banner ads.

On Friday, iDefense issued three security advisories that provided more information about some of the vulnerabilities that Adobe patched last week. Crediting iDefense researcher Greg MacManus with finding and reporting the bugs last September and October, the advisories said that the vulnerabilities were in Adobe Reader's handling of JavaScript and in how it refers to libraries that provide encryption and signature verification.

One of the two advisories that cited JavaScript flaws said there were "multiple stack-based buffer overflows in JavaScript methods" within Adobe Reader and Adobe Acrobat, a more advanced application that sells for US\$299 and up. "Exploitation of these vulnerabilities would allow an attacker to execute arbitrary code as the current user," the iDefense advisory said.

The Jan. 20 attack mentioned on the Italian forum exploited one of those JavaScript vulnerabilities. Presumably, the proof-of-concept exploit that Immunity researcher Kostya Kortchinsky crafted last week also took advantage of one of the iDefense-reported stack overflows. Immunity labeled the revised, fully-functional exploit as "JavaScript Stack Overflow" when it released it to CANVAS Early Updates subscribers on Thursday.

Symantec weighed in as well when one of its researchers, Hon Lau, said that the attacks in progress might have originated from malicious ads on hacked sites or from compromised legitimate sites that redirected users to a rigged PDF file via JavaScript or an iFrame. Attackers may also try to trick users into opening PDF files attached to spam, he added.

Although Lau did not cite specific figures, he put the victim tally as "many thousands" and warned users to patch Adobe Reader and Acrobat promptly. "It appears that this PDF-based attack has been quite successful affecting many thousands of users throughout the world," Lau said on the Symantec security blog Saturday.

Lau also speculated that details of the vulnerabilities had leaked before Adobe could patch them. "While it appears that the vulnerabilities were disclosed in a responsible manner, i.e. [the] vendor was informed and allowed to patch before official announcement, the swiftness of the exploit appearing in the wild could suggest that leaks had occurred," Lau maintained.

On Thursday, Adobe added a security advisory to its website, but the new alert did not provide any additional details on the vulnerabilities it had patched. In the advisory, Adobe credited iDefense's MacManus, as well as researchers at Google, Fortinet, 3Com's TippingPoint unit and Security-Assessment.com, a New Zealand-based security consultancy, for reporting the bugs.

The new Reader 8.1.2, which can be downloaded from the Adobe website or retrieved using the updater bundled with Reader, targets Windows and Mac OS X users. Adobe does not yet have a patched Version 7 of the application, but it said one would be made available at some point.

LATEST NEWS

Sinclair to leave Renaissance

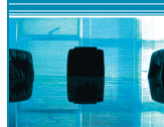
Telecom result helped by \$27m compensation payment

Gen-i awarded datacentre contract with Air New Zealand

FRY UP: They may be watching you

Five govt agencies engage with Public Records Act

Telecom revenue down, but some improvement seen



Do you have the best ICT project in the Government sector in New Zealand?

ENTRIES ARE NOW OPEN UNTIL 6 SEPTEMBER 2010.

CLICK HERE FOR MORE INFORMATION

PROUDLY SPONSORED BY:

SUBSCRIBE

Computerworld is New Zealand's only specialised information systems fortnightly. Subscribe now for \$97.50 (24 issues) and save more than 37% off the cover price!



SIGN UP

COMPENSATION OF COSTS

NAME: _____

EMAIL: _____

PHONE: _____

Get the latest news from Computerworld delivered via email. Sign up now

MOST POPULAR

READ COMMENTED EMAILED SHARED

- Netbook failure rate disappoints major user
- Google Wave code to live on
- Govt plans hinder FX Network sales
- File-sharing bill could extend surveillance culture - Bott
- Surveillance Bill amendments reassure telcos
- HP researcher cracks conundrum

WHITE PAPERS

- On Common Ground: Where Compliance and Data Protection Overlap
- Automation Makes Perfect: Taking the Time Crunch Out of IT Compliance with Automation

POPULAR EVENTS

- Excellence in the Use of ICT in Government Award 2010 Award
- The Sustainable 60 Awards
- The Sustainable 60 Workshops

SPONSORED LINKS

- Local and International news Enterprise ICT must know info
- NZ's most trusted tech advice

EMAIL PRINT SHARE THIS STORY WITH: