


{* SECURITY *}

Unpatched IE bug exploited in targeted attacks

'More than a few organizations' hit

By Dan Goodin 3 Nov 2010 at 18:06

11  SHARE ▼

Unknown attackers have been targeting a previously unknown vulnerability in Internet Explorer to take control of machines running the Microsoft browser, security watchers warned on Wednesday.

The exploits were hosted on a page of an unidentified website that had been breached without the owner's knowledge, according to antivirus provider Symantec, which discovered the attacks a few days ago. The perpetrators then sent emails that lured a select group of people in targeted organizations to the booby-trapped page, causing those who used IE versions 6 and 7 to be infected with a backdoor trojan.

The exploit required no interaction on the part of victims and gave no indication what was happening. While the exploit page was found on a single website, Symantec researchers warned the attacks may have been widespread.

"Looking at the log files from this exploited server we know that the malware author had targeted more than a few organizations," they wrote. "The files on this server had been accessed by people in lots of organizations in multiple industries across the globe."

In an encouraging sign, few of the visitors were affected because they weren't using a vulnerable browser, they added.

Version 8 of IE may also be vulnerable, but a security protection known as DEP, or data execution prevention – which is turned on by default – causes the browser to crash rather than to remotely execute the malicious code, Microsoft said. DEP, which was first added to IE 7, is designed to lessen the damage of such attacks by preventing data loaded into memory from being executed. While hackers have figured out ways to bypass the technology, so-called heap-spraying attacks don't work well with this particular bug.

The security flaw resides in a part of IE that handles CSS, or Cascading Style Sheets, tags. As a result, the browser under-allocates memory, allowing data to be overwritten in memory vtable pointers. By spraying memory with special data, an attacker can cause IE to execute code.

The report is the latest reminder of the benefits of moving to the latest version of IE – or to a different browser altogether. Those who must use IE versions 6 or 7, should consider augmenting it with EMET, Microsoft's tool for locking down older applications. It can be used to add DEP and other security mitigations to a variety of programs, including IE and Adobe Reader.

Microsoft didn't say when it planned to patch the vulnerability, but Jerry Bryant, a spokesman for Microsoft response, indicated the bug probably didn't warrant a release outside of the company's normal update cycle. That means the earliest we're likely to see a fix is December 14.

Microsoft has more details [here](#), [here](#) and [here](#). ®

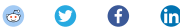
Sponsored: [Practical tips for Office 365 tenant-to-tenant migration](#)

Tips and corrections

11 Comments

 Sign up to our Newsletter - Get IT in your inbox daily

MORE Internet Explorer Zero Day Attack



// MOST READ

- 1 NASA to launch 247 petabytes of data into AWS – but forgot about eye-watering cloudy egress costs before lift-off
- 2 British Army adopts WhatsApp for formal orders as coronavirus isolation kicks in
- 3 Closed source? Pull the other one... We love open source, but not enough to share code for our own app, says GitHub
- 4 Forget James Bond's super-gadgets, this chap spied for China using SD card dead drops. Now he's behind bars
- 5 SpaceX beats an engine failure to loft another 60 Starlink satellites

SUBSCRIBE TO OUR WEEKLY TECH NEWSLETTER

SUBSCRIBE



// KEEP READING



If you never thought you'd hear a Microsoftie tell you to stop using Internet Explorer, lap it up: 'I beg you, let it retire to great bitbucket in the sky' We say take off and nuke the entire codebase from orbit. It's the only way to be sure



Disabled by default: Microsoft ups the ante in its war against VBScript on Internet Explorer Will the last IE 11 user please turn out the lights?



Edge, Internet Explorer users Czech their settings after MSN 'forgot' their language Surfers faced with challenging feeds on a new tab



Nine words to ruin your Monday: Emergency Internet Explorer patch amid in-the-wild attacks Update browser ASAP after Google gurus spot miscreants abusing bug to hijack PCs



Microsoft decides Internet Explorer 10 has had its fun: Termination set for January 2020 Windows Server 2012 admins should crank it up to 11



Microsoft adds Internet Explorer mode to Chromium Edge, announces roadmap Enterprise features including support for hated ancient browser ready to evaluate



It's Friday, the weekend has landed... and Microsoft warns of an Internet Explorer zero day exploited in the wild **ROUNDUP** Plus, WeLeakInfo? Not anymore!



'Supporting Internet Explorer is hell': Web developers identify top needs – new survey WebAssembly key tech for replacing native apps, say respondents

// TECH RESOURCES



Le Guide Des Échanges Transversaux Pour Les Entreprises En Croissance

L'équipe financière en tant que partenaire de l'entreprise



8 ways Legacy ERP Harms Businesses

Download this white paper to learn the 8 ways by which legacy ERP systems hold back your business and how "version-less" cloud ERP can help eliminate costly upgrades, reduce IT infrastructure management, and drive value with rapid implementation.



Executive Briefing: Kritische Gartner-Funktionen für Webanwendungs-Firewalls

An Akamai whitepaper



Secure Enterprise SD-WAN

Organizations are turning to SD-WAN as a cost-effective way to establish local internet breakouts and simplify traffic routing for the branch.

ABOUT US

Who we are
Under the hood
Contact us
Advertise with us

MORE CONTENT

Latest News
Popular Stories
Forums
Whitepapers
Webinars

SITUATION PUBLISHING

The Next Platform
DevClass
Blocks and Files
Continuous Lifecycle London
M-cubed



SITUATION PUBLISHING

The Register - Independent news and views for the tech community. Part of Situation Publishing

SIGN UP TO OUR NEWSLETTERS

Join our daily or weekly newsletters, subscribe to a specific section or set [News alerts](#)

SUBSCRIBE >

