The Register
Biting the hand that feeds IT

{* SECURITY *}

Nasty IE 0day exploit hosted on Amnesty International site

'Protecting human rights worldwide'

By Dan Goodin 11 Nov 2010 at 01:39

15 SHARE ▼

Visitors to Amnesty International's Hong Kong website are being bombarded with a host of lethal exploits, including one that attacks an unpatched vulnerability in Microsoft's Internet Explorer browser, researchers at security firm Websense said.

The injected IE attack code resides directly on the pages of amnesty.org.hk, an indication that the perpetrators were able to penetrate deep into the website's security defenses. The code exploits a vulnerability disclosed last week that gives attackers complete control over machines running default versions of IE 6 and 7. Version 8 isn't vulnerable, thanks to security protections built into the browser.

It's the second report in a week that the previously unknown vulnerability is being actively exploited to install malware on IE users' machines. Last week, antivirus firm Symantec warned that an undisclosed website had been compromised so that it was laced with code that targeted the flaw.

The attackers 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 underlying security bug resides in a part of IE that handles CSS, or Cascading Style Sheet, 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.

A security protection known as DEP, short for data execution prevention, prevents the attack from working. DEP is turned on by default in IE 8. Microsoft has advised those who must use IE 6 and 7 to use a security tool known as EMET to add DEP to those earlier versions.

Not that Microsoft or Amnesty International should be singled out. Last month, a zero-day vulnerability in Mozilla Firefox was exploited on the Nobel Peace Prize website.

The Amnesty International website is serving a variety of other exploits that attack previously patched vulnerabilities in Apple's QuickTime media player, and Adobe's Flash and Shockwave players. The Websense report is here. ®

Tips and corrections

15 Comments

MORE Microsoft Internet Explorer Vulnerability Exploit

// 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

// KEEP READING

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?

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

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!

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

Edge, Internet Explorer users Czech their settings after MSN 'forgot' their language

Surfers faced with challenging feeds on a new tab

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

Bill G on Microsoft's biggest blunder... Was it Bing, Internet Explorer, Vista, the antitrust row?

Nope: It was not giving Android a run for its money...

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

SIGN UP TO OUR NEWSLETTERS
Join our daily or weekly newsletters, subscribe to a specific section or set News alerts
SUBSCRIBE

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