Nasty IE 0day exploit hosted on Amnesty International site

By Dan Goodin

Published: 2010-11-11 · Archived: 2026-04-05 23:15:23 UTC

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. ®
