

## Emergency IE patch goes live as exploits proliferate

Microsoft released an emergency security update for all versions of Internet Explorer on Thursday as attacks exploiting a critical vulnerability in the widely used browser spread to hundreds of websites.

The patch fixing the IE vulnerability used to penetrate the defenses of Google and other large companies came as anti-virus provider Symantec said the flaw was being exploited on "hundreds of websites." While some of the sites hosting the attacks were free services that had been co-opted, others appeared to be domains of legitimate companies that had been compromised.

Microsoft said earlier Thursday that it continued to see "limited and targeted attacks against Internet Explorer 6 only." The company nonetheless strongly urged users to install the fix as soon as possible. While Talbot believes the attacks have now gone mainstream, he said none of the attacks he's seen in the wild are successful against versions 7 and 8, thanks to security features Microsoft has baked in to the browser.

The unscheduled bulletin fixes a memory corruption flaw in most versions of the widely used browser that allows attackers to execute malicious code simply by luring victims to a booby-trapped website. It fixes seven other privately reported vulnerabilities, some of which also made remote code execution possible, that Microsoft had been planning to issue next month during its next regularly scheduled patch release.

The update patches the holes by modifying the way IE handles objects in memory, validates input parameters, and filters HTML attributes. Although IE 5.01 isn't vulnerable to the exploits that penetrated Google, that version is susceptible to exploits targeting other bugs, so Thursday's patch is considered critical for all users.

Earlier this week, security firms including Websense and McAfee reported seeing copycat attacks that use the same code used against Google, but until now, those attacks appeared to be limited to a handful of websites that mostly targeted Chinese-speaking users. The new attacks are hosted on a variety of websites, including "well-known dynamic DNS hosting sites," Talbot said.

Systems compromised by the sites reported by Symantec were infected with a backdoor that collected registry settings and other system information and sent it to an email address that was under the control of attackers. That email address has since been disabled, Talbot said.

Virtual Technologies Group has taken charge and has deployed a patch to our Instant Help customers. For those of you who do not have our Instant Help feature, please contact your account representative to see how you can get on Instant Help or what you can do to help prevent your system from this virus. If you do not have an account representative, please contact [jmolnar@vtgus.com](mailto:jmolnar@vtgus.com) to be assigned one.

Lima location: 3820 S. Dixie Hwy. Lima, OH 45806 ♦ Phone: 419.991.4694 ♦ Fax: 419.991.4329

Toledo location: 19 N. Erie St. Toledo, OH 43604 ♦ Phone: 419.255.9070 ♦ Fax: 419.255.9762

[sales@vtgus.com](mailto:sales@vtgus.com) ♦ [www.vtgus.com](http://www.vtgus.com)