Tech Experts: 'Widgets' Are Huge Security Risk

Thursday , September 20, 2007

By Lisa Vaas

eWEEK.COM

Widgets — those fun, graphic little applications that bring things like clocks and calculators to your desktop — are all plagued with lousy security and stand ready to unleash the next wave of malware onto users' systems, according to new research.

The security holes in these applications already have opened up: Microsoft's MS07-048 advisory, put out on August's Patch Tuesday, addressed a vulnerability in Vista's Feed Headlines Gadget that could have let in malicious RSS feeds or links.

Apple patched its WebKit browser engine in June. WebKit serves as an engine not only for Safari but also for Dashboard — a set of widgets that delivers real-time weather, stock tickers, flight status and other information.

• Click here to visit FOXNews.com's Cybersecurity Center.

Now Finjan, a San Jose, Calif.-based security company, is reporting that new attacks exploiting widget and gadget insecurities in all types of environments — including operating systems such as Vista, third-party applications and Web widgets — are imminent and that the only thing that will stop the mayhem is a revised security model.

"All types of widget environments ... were found to be plagued with inadequate security models that allowed malicious widgets to run. In addition, we have found vulnerable widgets that were already available (some in the default installation) in the widget environment.

"These examples clearly show that the design and development of these mini-applications was missing some security considerations," the security company's Malicious Code Research Center reported in its Third Quarter Web Security Trends Report.

Finjan has been on this a while: Microsoft credits the security firm for its work behind the MS07-048 patch, and Finjan researchers Aviv Raff and Iftach Ian Amit presented a talk on the subject at the DefCon hacker conference on Aug. 5 titled "The Inherent Insecurity of Widgets and Gadgets."

Widgets and gadgets, Finjan says, are loosely based on Web models, such as HTML-like presentation and rendering and JavaScript-like APIs.

Unsurprisingly, the types of vulnerabilities they bring to a system are similar to those found on the Web. But widget and gadget engines magnify the threat, since they share a much broader connectivity with an underlying operating system, at least in the case of native-operating-system widgets and those from third-party widget engines.

This enables a powerful attack vector capable of gaining privileged access to local resources by default, Finjan says.

Finjan, located in San Jose, Calif., has found scads of security soft spots to date.

One that has since been fixed is a Contacts widget pre-installed in all flavors of Vista Sidebar. By providing a malformed, innocent-looking contact, an attacker could run code on a victimized system by simply having the contact displayed on the machine — no user interaction is required.

Another Microsoft soft spot is Live.com, a new, customizable portal that displays recent headlines from an RSS feed, a brief summary of a Hotmail account inbox, local weather forecasts and the like.

The RSS reader widget was vulnerable to swallowing malicious commands sent via data feed by attackers who could then gain access to privileged information from the user account, impersonating the user and taking over the browser.

Yahoo's widget engine is another one that has shown squishy security. That technology, based on Konfabulator, can be installed as a third-party application and will bring widget capabilities to operating systems that don't have a native widget engine.

At one point, Yahoo's widgets engine had a vulnerability in its Contacts widget that again allowed attackers to run through unsanitized script, Finjan says.

Finjan is expecting attacks via widgets and gadgets to ramp up, particularly given their ubiquity — they're found on iGoogle, Live.com, Yahoo, Vista and on Mac operating systems.

Finjan's MCRC is recommending that users stay away from nontrusted third-party widgets and that they be treated as full-blown applications, with all the power to own a system that that implies.

They're also recommending caution when using interactive widgets, given that their reliance on external feeds such as RSS or weather information might open the door to attacks that piggyback malicious payloads onto trusted content.

As for security policy, Finjan wants to see strict policies around widgets and widget engines.

"Since these are not considered business critical applications, or even productivity enhancers in some cases, the use of widgets and gadgets by corporate users should be limited," the MCRC says in its report.

Also, widgets and gadgets should be blocked at the gateway, Finjan says, to keep them off corporate networks.

"Vendors and users alike must realize that every application — even if it's small and made mostly for the sake of visual entertainment — represents a potential security threat," the MCRC says in its report. "Vulnerabilities in widgets and gadgets enable attackers to gain control of user machines, and thus should be developed with security in mind, so that users can enjoy the benefits of these advancements.

"This attack vector could have a major impact on the industry, immediately exposing corporations to a vast array of new security considerations that need to be dealt with. Businesses require security solutions [that] are capable of coping with such a changing environment, analyze code in real time, and detect malicious code appearing in such innovative attack vectors can provide adequate protection for these businesses."