Computerworld, Microsoft scrambles as it patches 26 bugs, warns users of active attack (6.13.12)

Microsoft scrambles as it patches 26 bugs, warns users of active attacks

Hectic, info-packed Patch Tuesday as software maker yanks update, patches worm-ready flaw and tells customers to get some fixes manually

Gregg Keizer

June 13, 2012 (Computerworld)

Microsoft on Tuesday patched 26 vulnerabilities, including one in Internet Explorer (IE) that's already being exploited. The company also warned customers of a new zero-day attack and quashed yet another instance of a bug that the Duqu intelligence-gathering Trojan leveraged.

The software maker also ditched one security update at the last minute and substituted another in its place, probably because the second was more serious.

Of Tuesday's seven security updates, three were rated "critical," Microsoft's top-most threat ranking, while the other four were marked "important," the next-most-serious label.

The 26 vulnerabilities -- one more than Microsoft last week told users to expect -- included 10 critical, 14 important and two judged "moderate" in the company's four-step scoring system.

Independent researchers almost unanimously pegged MS12-037 as the update Windows users should grab first.

The 13-bug patch collection affects all versions of IE, including IE10 on Windows 8 Consumer Preview, the February sneak peak that was superseded by the Review Preview two weeks ago.

"It's always important to get an IE update deployed," said Jason Miller, manager of research and development at VMware, as he cited the browser's popularity, especially in business, and thus the huge number of possible victims.

Microsoft admitted that one of the baker's dozen was already being exploited by hackers, raising the importance of applying the update immediately. "Microsoft is aware of limited attacks attempting to exploit the vulnerability," stated the company's advisory, which divulged no other details of the ongoing exploits. The vulnerability affects only IE8, the 2009 version that remains the most widely used version of Microsoft's browser.

A second vulnerability patched by MS12-037 has been publicly disclosed, Microsoft said.

Also included in the 13 was a critical vulnerability that French firm Vupen Security exploited to hack IE9 at March's Pwn2Own contest, where researchers face off against browsers for cash prizes. For its efforts, which featured a hack not only of IE9 but also Google's Chrome, the Vupen team took home $60,000.

Last week, Andrew Storms, director of security operations at nCircle Security, bet that the Vupen bug would be patched this month. But Tuesday, he said it was too close to call between the IE update and a rival, MS12-036, for first-to-fix honors.

"Certainly, [MS12-036] makes it to the top of the worrisome list," said Storms.

That update, also rated critical, patches just one vulnerability in the Remote Desktop Protocol (RDP), a Windows component that lets users remotely access a PC or server. RDP is frequently used by corporate help desks, off-site users and IT administrators to manage servers at company data centers and those the enterprise farms out to cloud-based service providers.

Most researchers were worried about the RDP bug.

"This is potentially wormable," said Storms.

"Definitely wormable," echoed Miller.

The vulnerability, dubbed CVE-2012-0173, could be exploited by an attacker who simply sends specially crafted data packets to a system with RDP enabled, said Microsoft. All versions of Windows, both client and server, are affected, ranging from Windows XP SP3 to Windows 7 SP1.

Researchers had a sense of deja vu.

Microsoft patched a very similar RDP vulnerability in March with the MS12-020 update. At the time, Miller said he was "spooked" by the bug and its potential exploit in a network-attacking worm. Storms said it "had all the ingredients for a classic worm."

But there was more to the story: Just three days later, Italian vulnerability researcher Luigi Auriemma, who in May 2011 had discovered one of the just-patched RDP bugs, accused Microsoft of leaking his proof-of-concept (PoC) attack code to Chinese hackers.

Auriemma had submitted that PoC to a Hewlett-Packard bug bounty program to demonstrate the flaw; HP had in turn passed it along to Microsoft.

But Auriemma found the exact same code on Chinese forums and websites, some of them known hacker hangouts.

Seven weeks later, Microsoft tossed one of its Chinese partners, Hangzhou DPTech Technologies, from an information-sharing program it hosts for scores of antivirus firms. Microsoft said that DPTech had "breached our non-disclosure agreement" as it pinned the leak on the firm.

"It looks like Microsoft investigated further after patching the bugs in March and found this one," said Storms.

Amol Sarwate, manager of Qualys' vulnerability research lab, agreed. "Actually, this is quite common," said Sarwate of Microsoft's discovery of another flaw in code proven to have a vulnerability.

Theoretically, enterprises using RDP would have followed Microsoft's advice in March to lock down their networks by blocking ports at the firewall or enabling Network Level Authentication, or NLA, to force authentication before an RDP session begins. Doing so would block exploits of both the March and June bugs.

Miller wasn't optimistic IT administrators had done that. "Unless the mitigations come through with a patch, they're hard pressed for time to do it manually," Miller said. "But RDP should only be available to machines on your local network."

Exactly, added Pierluigi Stella, chief technology officer at Network Box USA, a Houston-based Internet security firm.

"In over 10 years in this job, I still cannot fathom why someone would open [the RDP] port to the Internet without the protection of a VPN or remote connection software like Citrix," said Stella in an email Tuesday. "Nevertheless, even within our customers, we count several who demanded this port be open from the Internet, despite our strong advice against it."

Other security updates from Microsoft patched flaws in the .Net framework, the company's Lync enterprise instant messaging product, Windows' kernel and kernel mode drivers, and its Microsoft Dynamics AX 2012, an enterprise resource planning (ERP) program.

Some of those need close inspection, said Miller.

"If you don't review [MS12-039 and MS12-040] you could miss something," Miller said. "Quite often we just assume our patch management product will cover all products and patches, [but] it is important to stay vigilant and read all information that is released to ensure your network is 100% covered."

Miller was referring to footnotes in those bulletins that told customers that some (in the case of MS12-039, the Lync update) and all (for MS12-040, which affects Dynamics AX) of the patches must be downloaded manually from Microsoft's Download Center. They're not served up through the usual Windows Update service or the enterprise-grade Windows Server Update Service (WSUS) software.

The Lync update had its own back story that intrigued researchers.

One of the vulnerabilities patched in MS12-039 had been fixed several times in other Microsoft software, first in November 2011, then again in May 2012. In each case, the bug was located in code that parsed TrueType fonts.

Last month, Microsoft acknowledged that the code had been copied and pasted into multiple products, and said it was hunting down each occurrence.

What was noteworthy about the font-parsing code was that it had been exploited last fall by Duqu, a sophisticated cyber-spying Trojan that most experts believe was linked to the even-more-notorious Stuxnet, the worm used to sabotage Iran's nuclear program in 2009 and 2010.

"Microsoft has done a source code audit to find instances where this [font parsing code] was in use," said Wolfgang Kandek, chief technology officer at Qualys. "This month's might be a leftover of that audit."

Storms speculated that Microsoft added MS12-039 at the last moment -- the Lync update had not been mentioned in last week's advance notification -- because of the ties to Duqu.

Another expert, Marc Maiffret, chief technology officer at BeyondTrust, chided Microsoft for the constant patching of the same bug.

"Here we are seven months after the original Duqu fix for TrueType font parsing and this same code reuse bug has reared its ugly head [again]," said Maiffret in an email.

In fact, the Lync update took the place of one that Microsoft had intended to ship Tuesday, but pulled for some reason. The company did not explain why it yanked that update, which was to patch all versions of Microsoft Office on Windows, but when it's made last-minute changes before, it's been because it found a flaw in the update or encountered compatibility issues with its own or important third-party software.

Researchers, including Storms, expect that Microsoft will ship the delayed Office update next month.

Microsoft also issued a new security advisory on Tuesday, admitting that a critical unpatched vulnerability in all versions of Windows -- as well as in Office 2003 and Office 2007 -- was being exploited by attackers who duped victims into visiting malicious websites.

"Our investigation is underway," said Angela Gunn of Microsoft's Trustworthy Computing team in a blog post Tuesday.

Until a patch is ready, Gunn urged customers to run the free "Fixit" tool Microsoft made to block attacks aimed at IE users.

Google, whose security team uncovered the attacks, and along with a Chinese security company, reported the bug to rival Microsoft, reiterated Gunn's advice in a blog post of its own Tuesday. It also offered a bit more information than Microsoft.

"These attacks are being distributed both via malicious Web pages intended for Internet Explorer users and through Office documents," said Andrew Lyons, a Google security engineer.

Microsoft did not set a delivery date for a patch, but Miller said he wouldn't be surprised if the company went "out-of-band" and released an emergency update for Windows and Office before July 10, the next scheduled Patch Tuesday.

June's seven security updates can be downloaded and installed via the Microsoft Update and Windows Update services, as well as through WSUS.

metatag data Patch Tuesday, Microsoft, Windows, Internet Explorer, IE, Windows 8 Consumer Preview, Gregg Keizer, Andrew Storms, cyberwarfare, Stuxnet, Duqu, Wolfgang Kandek, Jason Miller, Google, Chrome, Office, zero-day, out-of-band, worm, RDP,