MS Patch Tuesday Fires Off 14 Critical Updates

May 9 2007

System administrators will have to prioritize between updating Exchange and DNS servers while leaving equally important server and application updates dangling, experts say.

Microsoft has released patches for 19 vulnerabilities, 14 of which are critical, hitting at holes in Excel, Word, Office, Exchange, Internet Explorer, cryptographic technology and the whopper of them all, the zero-day vulnerability in the DNS Server's use of RPC.

Michael Sutton, a security evangelist for Atlanta-based SPI Dynamics, said the "pretty high percentage" of critical updates on this Patch Tuesday is going to force a lot of system administrators to juggle updates, making decisions about which servers to update first. System administrators "can't take care of everything at once," he said. "You have to look at severity."

Sutton said he's advising people to first focus on the Exchange and Domain Name System updates, given that those vulnerabilities will leave companies the most exposed to attack. " [It's a] challenge; when you have 14 criticals, you're putting some things secondary that are still top priorities," he said.

An exploit for the DNS RPC (remote procedure call) interface vulnerability was discovered in the wild in April. Within a week of its discovery, four new malicious programs popped up, each trying to take over systems by prying open the DNS hole.

The DNS remote code execution vulnerability affects server-grade operating systems, including Windows 2000 and Windows Server 2003, and only those that have the DNS service enabled, such as Domain Controller, DNS Server or Microsoft Small Business Server configurations.

Still, warned Symantec, based in Cupertino, Calif., enterprises and small businesses "should ensure [that] they update their systems with the patch since this vulnerability has already been exploited." A successful exploit would completely compromise the computer.

"As we reported in the recent Internet Security Threat Report, attackers are continuing to leverage browser and application vulnerabilities and social engineering tactics to gain access to computers in order to execute malicious code," Oliver Friedrichs, director of emerging technologies for Symantec Security Response, said in a statement. "It is important that users protect themselves by updating their computers with recent patches, using common sense when connecting to the Internet and installing a comprehensive security suite."

Windows customers should immediately apply the DNS update, Microsoft said, to avoid the possibility of remote attackers hijacking their systems. The patch can be downloaded here.

Another one of the most critical of the security updates, security bulletin MS07-026, affects Microsoft Exchange. It addresses a remote code execution vulnerability that affects the MIME (Multipurpose Internet Mail Extension) decoding mechanism of Microsoft Exchange Server 2000/2003/2007. The vulnerability can be triggered by a malformed base64-encoded attachment.

The update covers several newly discovered Exchange vulnerabilities that have been privately reported. Sutton said he's guessing that the

Exchange issue with MIME could well be an internal find on Microsoft's part, which means that the exploit might not be in the wild anytime soon.

"In that advisory, it's interesting that three people are credited for three different vulnerabilities, and the only one that doesn't get credited is [the MIME vulnerability]," he said.

Microsoft said the most severe of the Exchange holes could allow a successful attacker to gain complete control of a system, after which he or she could install programs, view, change or delete data, or create new accounts with full user rights.

Symantec said a successful attack depends on an Exchange user opening a malformed attachment. A compromised machine that hosts a vulnerable Exchange server could affect a large number of people, Symantec pointed out.

Because Exchange is such a critical communication vector, this update could have wide impact for companies that haven't worked out plans to roll out the patch midweek. Many companies rely on waiting until the weekend to patch Exchange because of the business disruption that comes from taking down e-mail servers. If an exploit surfaces between now and then, such companies could be in serious trouble.

Don Leatham of PatchLink, based in Scottsdale, Ariz., said in an interview the week of April 30 that were this Exchange patch to involve remote code execution, it could have a serious impact on companies' patch schedules. That, in fact, is the case.

One PatchLink customer, Richard Linke, said in an interview the week of April 30 that he would be rolling out Exchange updates following the sun, using Australia as the guinea pig. "You can't take all - the Exchange servers - out at once, or everybody winds up not being able to do mail,"

said Linke, an independent security consultant and former global security manager at Kraft Foods.

Linke will be overseeing the update of 36 Exchange servers around the world. As far as the other security and non-security updates go, he's looking at updating 5,000 servers.

Linke said, "[We'll] notify regions of what times [we'll] plan to do it. As the sun rises in one place, - we'll make sure the - Exchange group server is done."

Microsoft recommends updating immediately, and the patch can be downloaded here.

Sutton also noted "a ton" of file format vulnerabilities, both on this Patch Tuesday and cumulatively over the past 18 to 24 months. For example, an attacker will send a malformed Word or Excel file. Such files are used so commonly in the business world, Sutton said, that an attacker has a "decent chance of somebody opening that file and being exploited."

" [File format vulnerabilities] are something Microsoft is still struggling with," Sutton said.

Three of the critical vulnerabilities addressed in the May 8 security updates are illustrative of the file-format vulnerability trend. Those three are remote code execution problems found in Excel: a BIFF Record Vulnerability, an Excel Set Font Vulnerability and an Excel Filter Record Vulnerability. The Excel update can be found here.

Another three critical remote code execution vulnerabilities that illustrate file-format problems have been patched in Word: a Word Array Overflow Vulnerability, a Word Document Stream Vulnerability and a Word RTF Parsing Vulnerability. The updates can be found here.

Microsoft is also tackling six critical vulnerabilities in Internet Explorer. The vulnerabilities are found in a range of IE iterations, from IE 5.01 SP4 running on Windows 2000 SP4 on up to IE 7 on Windows Vista. Also affected are IE 6 SP 1 when installed on Windows 2000 SP4, IE 6 for Windows XP SP 2, IE 6 for Windows Server 2003 SP1 and SP2, IE 7 for Windows XP SP2, and IE 7 for Windows Server 2003 SP1 and SP2.

The vulnerabilities consist of a COM (Component Object Model) Object Instantiation Memory Corruption, an Uninitialized Memory Corruption, a Property Memory Corruption, an HTML Objects Memory Corruption and an Arbitrary File Rewrite. The cumulative update can be found here.

Microsoft has also addressed a critical vulnerability in the CAPICOM (Cryptographic API Component Object Model) and BizTalk that could allow remote code execution. The update can be found here.

Finally, Microsoft has patched one critical remote code execution vulnerability found in Office. This problem, which could also allow for complete system takeover, concerns a Drawing Object vulnerability - yet another file-format vulnerability. The update can be downloaded here.