

2007/02/05

Vista exploitable, researcher says

SAN FRANCISCO -- It's possible to elevate system privileges by exploiting a flaw in Microsoft's newly released Windows Vista operating system, according to one well-known vulnerability researcher.

Marc Maiffret, CTO and chief hacking officer of Aliso Viejo, Calif.-based eEye Digital Security Inc., said during an interview at RSA Conference 2007 Monday that according to his research, there's a way to use a non-Microsoft vulnerability to remotely compromise Vista, as well as a way to elevate system privileges using a Vista-specific flaw.

He will demonstrate his findings later this week at the IT-Defense 2007 conference in Leipzig, Germany.

"This is a vulnerability specific to Vista that doesn't even exist in XP," Maiffret said. "With Vista they've done a lot of things [to improve security], but mistakes are still there."

This isn't the first time a security expert has warned of a flaw in Vista. In December, Microsoft acknowledged it was investigating claims that attackers could boost system privileges and run malicious commands by targeting an issue with the Windows Client/Server Runtime Server Subsystem (CSRSS). That issue reportedly affected Vista and other versions of Windows.

Maiffret was asked about Vista during a wider discussion about today's security threats and how well vendors are responding to them. Vista issues aside, he said Microsoft has come a long way in improving the security of its products. He said Microsoft was forced to take security more seriously because IT professionals got fed up and demanded action. He said vulnerability researchers must now educate IT professionals on security threats affecting other vendors. Once educated, he said, IT professionals can put pressure on other vendors to do better, just as they did with Microsoft.

"As a researcher, you want to keep the vendor honest," he said. "The way to do it is to keep IT people on your side by educating them. If you really want to drive Apple or another vendor to do better, that's the number-one way to do it."

Searchsecurity.com 05.02.07



cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de