Naughty Norton: Symantec Fixes Flaw in Security Software

May 18 2007

The security vendor has patched a buffer overflow vulnerability that could allow an attacker to remotely execute malicious code.

Symantec has fixed a serious vulnerability with an ActiveX control used by Norton Personal Firewall 2004 and Norton Internet Security 2004 that could allow a hacker to execute code remotely on a vulnerable system.

According to Symantec officials, the company was notified of the problem by US-CERT. A buffer overflow can be triggered by an error that occurs in the Get () and Set () functions used by ISAlertDataCOM, part of ISLALERT.DLL. Successfully exploiting this vulnerability would allow an attacker to remotely execute malicious code on an unpatched system and give them the rights of the logged-in user, Symantec officials said.

In order for an exploit to work, however, the hacker must first trick the user into viewing a specially crafted HTML document. As noted in the advisory, such attacks frequently begin with an e-mail containing a link to the malicious site that is meant to entice the user.

"Symantec product engineers have determined that the issue affects Norton Personal Firewall and Norton Internet Security 2004 only," the advisory states. "Product updates to correct the problem are available through LiveUpdate."

Though the company lists the threat as medium, it is rated highly critical by Secunia. Symantec officials said they are not aware of any customers impacted by the flaw, or any attempts to exploit it, and recommend users keep their patches up to date. A plug for the security hole can be obtained through Symantec's LiveUpdate feature.