Security Certificate Issues Plague Dell

By David Jones
Nov 28, 2015 10:45 AM PT

Print
Email

Dell earlier this week announced that it was notified of a security flaw linked to a certificate that it installed on computer systems starting on Aug. 18.

The eDellroot certificate was installed by Dell Foundation Services application as a means to help users more easily perform maintenance and service tasks on their computers, the company said.

The certificate is not malware or adware, according to Dell. Rather, it was provided with a download designed to provide a system service tag to Dell online support, which would allow quick identification of the computer model of the individual device.

"Unfortunately, the certificate introduced an unintended security vulnerability to systems -- both consumer and commercial -- in use by customers," said Dell spokesperson Christina Maria Furtado.

The certificate was added on some new systems at the factory between Nov. 20 and Nov. 23, she told TechNewsWorld, and the company planned to push a software update to get rid of the problem on those systems.

Dell posted instructions on its website to permanently remove the certificate, and also added that it would post a software update to check for the certificate automatically, and if found, to remove it from affected systems.

Commercial customers who re-imaged their systems without Dell Foundation Services were not impacted by the flaw, Dell said.

Dell publicly thanked three users who brought the flaw to their attention -- Hanno Bock, Joe Nord and Kevin Hicks, aka "rotocowboy."

Nord first discovered the flaw last weekend, in a Dell Inspiron 5000 series notebook purchased last month.

Lenovo Reminder

Dell's certificate problem is similar to a Superfish-type vulnerability that hit Lenovo systems earlier this year.

In that incident, Lenovo preloaded a type of spyware that basically allowed users to bypass HTTPS security.

"The core problem here is that the certificate that was shipped with these machines includes its own private key," noted Kevin O'Brien, founder and chief executive of GreatHorn.

The danger of this type of security flaw is that the attacker can intercept and decrypt Web traffic without the victim's knowledge. Any machine with the certificate is a potential target, he told TechNewsWorld.

The Dell case likely resulted from an oversight, O'Brien said, but it still highlights the need for a very fast response, both on the part of Dell and its customers.

"Dell is generally a responsible vendor, and I would expect to see them address this both in the short term via a fix and over the longer term by increasing their security review process," he added, "ideally with more automated analysis over all potential threat surfaces."

Security Flaw Fallout

The Dell security flaw resulted in false certificates showing up in unexpected and very vulnerable places, noted Andrew Lewman, vice president of data development at Norse.

"There are already fake Google certs out there signed by the eDellRoot certificate authority," he told TechNewsWorld. "This could mean when logging onto a bank, secure legal portal, Gmail, etc., that a criminal can easily grab the username and password entered into the desktop or laptop browser and see all of the traffic between the browser and the server."

As a matter of security, enterprises should block the Dell certificate authority both on the network and on individual devices, Lewman said.

Dell should be commended at least for not trying to deny the flaw, said Ian Trump, security lead at LogicNow. [*Correction - Nov. 30, 2015]

What Dell did wasn't malicious or intentional in his view, and the company clearly was doing everything it could to be transparent about the process, he told TechNewsWorld.

"It's encouraging to see vendors adopt technologies to secure communication and authenticate messages," Trump said. "The problem is, cryptography is hard -- and if cyberskills are in short supply, specialists in programming secure, encrypted communications are even harder to find."

Editor's Note: As Dell scrambled to resolve the eDellroot certificate problem, news of a second certificate issue surfaced on Wednesday. The optional Dell System Detect application and its DSDTestProvider root certificate had similar characteristics to eDellRoot, the company acknowledged. The Dell System Detect flaw affected customers who used the "detect product" functionality on the Dell support site between Oct. 20 and Nov. 24. Dell removed the application on Tuesday, replacing it with a version without the problematic certificate. ECT

***ECT News Network editor's note - Nov. 30, 2015:** Our original published version of this story incorrectly identified LogicNow's Ian Trump as Ian Smith. We regret the error.

David Jones is a freelance writer based in Essex County, New Jersey. He has written for Reuters, Bloomberg, *Crain's New York Business* and *The New York Times*.

Reader Comments

Be the first to comment!