InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

11/24/2015
12:00 PM

Ericka Chickowski
News
Connect Directly

0
COMMENTS
COMMENT NOW

Login

50% 50%

Tweet**Dell Hands Hackers Keys To Customer Systems**

Dell installs root certificate with associated private keys to create its very own Superfish scenario.

Dell customers are scrambling today to deal with a root certificate debacle that some security experts are likening to the Lenovo Superfish issue that emerged earlier this year. Brought to light in a reddit post over the weekend, the issue is with a root Certificate Authority (CA) certificate called eDellRoot that includes a private key and has been installed on new Dell computers and those updated by Dell software.

"It's not a simple bug that needs to be fixed, it's a drop-everything and panic sort of bug," wrote Rob Graham, owner of Errata Security. "Dell needs to panic. Dell's corporate customers need to panic."

According to the researchers with Duo Labs, the fact that eDellRoot is being shipped with an associated private key that is identical in all models is an epic fail. This information makes it trivial to impersonate websites, whether it be online banking sites, shopping sites, or Google.

"If a user was using their Dell laptop at a coffee shop, an attacker sitting on the shop’s wi-fi network could potentially sniff all of their web browsing traffic, including sensitive data like bank passwords (or) emails," wrote Duo Labs researchers Darren Kemp, Mikhail Davidov and Kyle Lady. "The attacker could also manipulate the user’s traffic, e.g., sending malware in response to requests to download legit software, or install automatic updates - and make it all appear to be signed by a trusted developer."

According to Graham, if he were an attacker, he'd be out at the nearest big city airport by the international first class lounges and eavesdropping on encrypted communications in hopes of finding vulnerable Dell users.

"I suggest 'international first class,' because if they can afford $10,000 for a ticket, they probably have something juicy on their computer worth hacking," Grahm says.

For its part, Dell acknowledged the issue yesterday and posted instructions on how to remove the certificate from its machines. As of today, Dell software updates will remove the certificate, the company says. Dell also says that unlike with Lenovo, the root certificate was not used to insert adware on customer machines.

"The certificate is not malware or adware. Rather, it was intended to provide the system service tag to Dell online support allowing us to quickly identify the computer model, making it easier and faster to service our customers," Dell said in a statement. "This certificate is not being used to collect personal customer information."

This really doesn't matter to the security community, though. While the fact that Superfish was meant to power adware made things worse, Graham says that the big problem was a root cert shipping with private keys.

"In this respect, Dell's error is exactly as bad as the Superfish error," he says.

According to Andrew Lewman, vice president of data development at Norse, enterprises should automatically be reinstalling operating systems rather than trusting default factory installs. Nevertheless, they should take extra precautions.

“As for protection, all enterprises should block the Dell certificate authority both on the network and on their devices. Uninstalling the certificate authority from laptops and desktops should be a matter of a policy update.”

Ericka Chickowski specializes in coverage of information technology and business innovation. She has focused on information security for the better part of a decade and regularly writes about the security industry as a contributor to Dark Reading. *View Full Bio*

COMMENT | EMAIL THIS | PRINT | RSS