Sloppy Security Software Exposes Dell Laptops to Hackers

By Paul Wagenseil, SecurityNewsDaily Managing Editor | November 23, 2015 11:30 pm

Dell may be selling some Windows laptops with a dangerous security flaw that could allow hackers to access your computer. Users have reported that recent-model Dell laptops, including the XPS and Inspiron 5000 series, come preloaded with self-signed digital certificates that could let criminals and spies impersonate Dell and upload malware to these PCs, which could do anything from stealing your personal information to turning your computer into a bot.

A thread on Reddit appeared earlier today (Nov. 23) detailing Reddit user Rotorcowboy's discovery of a Dell certificate, called eDellRoot, upon a recently made XPS 15 laptop. Rotorcowboy discovered that the certificate contained a private key, and was able to extract it using commonplace hacker tools. On a recently made Dell XPS 13, we found a second self-signed certificate, called DSDTestProvider, that also contained a private key -- a big security mistake.

Anyone with a recent Dell laptop can test for the presence of the eDellRoot certificate by visiting https://bogus.lessonslearned.org/, which uses that private key to authenticate itself as Dell. If you see an image of a ninja dog, you might be in trouble.

MORE: Best Midrange PC Antivirus Software

"If I were a black-hat hacker, I'd immediately go to the nearest big-city airport and sit outside the international first-class lounges and eavesdrop on everyone's encrypted communications," wrote Robert Graham, chief technical officer of Atlanta-based Errata Security, in a blog posting. "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."

Graham means that anyone could use the Dell certificate's private key to stage man-in-the-middle attack upon other computers on the same public Wi-Fi network. With Dell's private

But the attacks need not be limited to a single Wi-Fi network. Malicious websites could impersonate Dell, then upload bogus Dell software to Dell machines; malicious online ads could do the same thing even on benign websites.

Ars Technica said that some Inspiron 5000 laptops might also be affected.

Second Bad Certificate Found

Here at Laptop Mag, we found both the eDellRoot and the DSDTestProvider certificates on a new Dell XPS 13 laptop; they shared the same expiration date of Nov. 9, 2031. Like eDellRoot, DSDTestProvider was also self-signed and contained a private key. A two-year-old Dell XPS 13 also in our possession did not contain either certificate.

It's not clear what either certificate is for, but some Reddit users speculated they might be in-house production certificates that accidentally made their way into a retail build of Windows. Earlier this year, Lenovo was found to be installing self-signed certificates as part of the "Superfish" ad-injection software, which made Lenovo a little extra cash; there's no indication that the Dell certificates are part of a similar program.

"Customer security and privacy is a top concern for Dell," a Dell spokesman told us. "We have a team investigating the current situation and will update you as soon as we have more information."

Other tech websites received more detailed explanations, which a Dell spokesman confirmed were accurate.

"The recent situation raised is related to an on-the-box support certificate intended to provide a better, faster and easier customer support experience," CSO's Steve Ragan quoted a Dell spokesman as saying. "Unfortunately, the certificate introduced an unintended security vulnerability. To address this, we are providing our customers with instructions to permanently remove the certificate from their systems via direct email, on our support site and Technical Support."

"We began loading the current version on our consumer and commercial devices in August to make servicing PC issues faster and easier for customers," a Dell spokesman apparently told Ragan's IDG colleague Jeremy Kirk. "When a PC engages with Dell online support, the certificate provides the system service tag allowing Dell online support to immediately identify the PC model, drivers, OS, hard drive, etc. making it easier and faster to service. No personal information has been collected or shared by Dell without the customer's permission."

How Digital Certificates Work

Digital certificates are used to verify authenticity on the Internet, making certain that the website to which you connect really belongs to, for example, Amazon, or that software you download really comes from Microsoft. But they have to be properly implemented, and it appears that the eDellRoot certificate wasn't.

Here's a somewhat brief explanation. Digital certificates work using public-key cryptography, in which one party distributes a public key (really a very long prime number), but keeps secret a private key (also a very long prime number) that is mathematically linked to the public key. Any message encrypted with the private key can be decrypted by the public key.

When a Web browser connects to a secure (HTTPS) website, the website sends a message encrypted using its private key. The browser decrypts the message using the public key in the


Faulty iPad Pros May Lock Up After Charging


How to Stop Windows Update from Automatically Restarting Your PC


How to Use Offline Maps in Windows 10

But to maximize the security of this system, the certificates themselves should be certified by a "higher power," a third party trusted by all that verifies that the digital certificate is genuine.

If this all sounds complicated and boring, it is. But without digital certificates, you wouldn't be able to trust shopping or banking sites, or software updates delivered over the Internet.

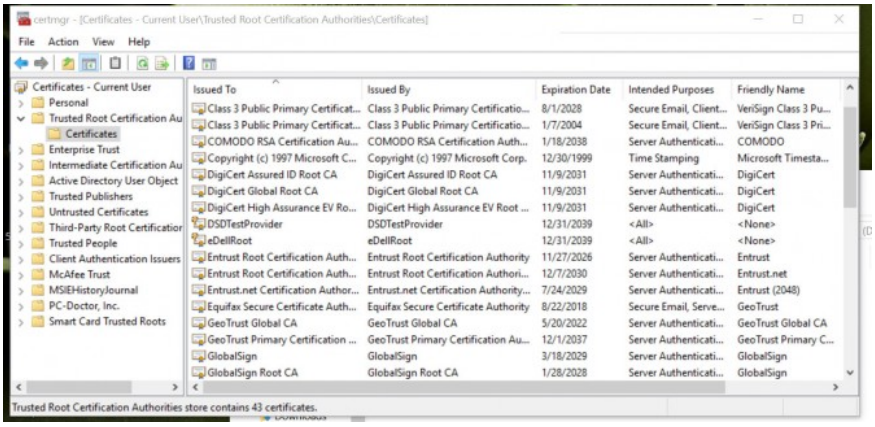
Undermining Your Security

The problems with the eDellRoot and DSDTestProvider certificates is that they each contain both a public and a private key, and list themselves as the higher authority guaranteeing authenticity — hence, they're "self-signed." You could extract the private key from either, use it to certify a bogus website, wait for affected Dell laptops to initiate secure Web sessions and — bingo! — infect those laptops with malware.

"Anyone can impersonate Dell" using the eDellRoot certificate, Andrew Lewman, vice president of data development at Foster City, California-based security consultancy Norse, said in a statement. "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."

How to Remove the Certificates

IT personnel are trained to uninstall digital certificates, but it's not so difficult to do it yourself. If you have administrative rights on a Windows PC, go to the Start menu, type in "certmgr.msc," click "Trusted Root Certification Authorities," then click "Certificates." If you have a certificate named "eDellRoot" or "DSDTestProvider," right-click it, delete it, and restart the computer.



- 10 Worst Data Breaches of All Time
- 12 Computer Security Mistakes You're Probably Making
- Best Antivirus Protection for PC, Mac and Android

ADD A COMMENT

Email

Name

Comment

SUBMIT

Back to top

COMPANY

- Company Info
- About the Site
- Contact Us
- Advertise with Us
- Using Our Content
- Licensing & Reprints
- Copyright Policy
- Terms of Use and Sale
- Privacy Policy

NETWORK

- Top Ten Reviews
- Tom's Guide
- Laptop Mag
- Tom's Hardware
- Business News Daily
- Tom's IT Pro
- Space.com
- Live Science

FOLLOW US

SUBSCRIBE TO LAPTOP

enter email here ....

SUBMIT