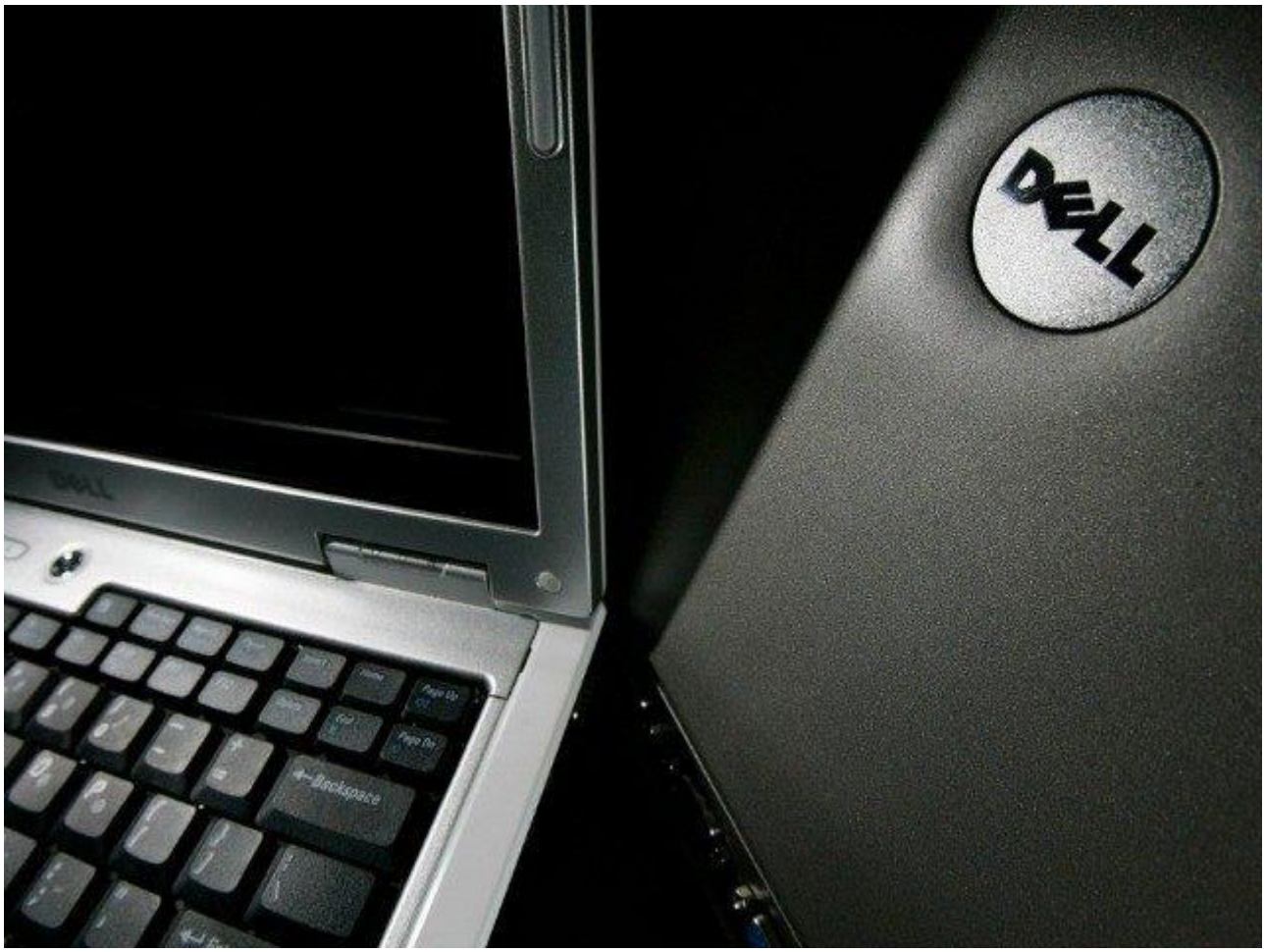
Dell Compromises Customer's Security with Pre-installed Rootkit



By *Nate Church, 24 Nov 2015*

The alarm was sounded first — as usual — on Reddit. Soon Twitter and various blogs by users and security experts chimed in to support the findings. Apparently, Dell has been shipping computers loaded with a self-signed root digital certificate.

In layman's terms, Dell taped an extra car key to the front fender and left it there without telling anyone who bought it. In fact, this security certificate isn't even unique for each computer. That means that any nominally motivated attacker can gain access to a digital "signature" that would allow them to perfectly impersonate, say, Google. They can then open an encrypted channel directly to your data with not so much as a twinge from any installed security measures.

"eDellRoot" has been spotted on models from the Inspiron, Precision, and Latitude lines of Dell PCs. It's not totally clear how widespread the implementation has been, but the evidence is already overwhelming. Duo, an online security service, published a report on their findings related to the scandal.

In response, Dell has issued a statement in which they assert, "Customer security and privacy is a top concern and priority for Dell; we deeply regret that this has happened and are taking steps to address it."

Earlier this year, Lenovo ran into the same trouble over pre-installed Superfish adware that opened similar vulnerabilties. While they claimed not to have found "any evidence to substantiate security concerns," they very quickly stomped the brakes on its usage.

Dell says they will be providing consumers with instructions for how to remove their rootkit, but tinkering with digital licenses is beyond the savvy of the average consumer. With a universal key to private data lying out there for any would-be invaders, the response could be too little, too late.

Nate Church is @Get2Church on Twitter, and he can't become a wildly overhyped internet celebrity without your help. Follow, retweet, and favorite everything he says. It's the Right Thing To Do™!

Security

Dell: How to kill that web security hole we put in your laptops, PCs

Promises to automatically remove root CA cert from machines from Nov 24

24 Nov 2015 at 01:14, Chris Williams

Dell has published a guide on how to remove the web security backdoor it installed in its Windows laptops and desktop PCs.

This confirms what we all know by now – that Dell was selling computers with a rather embarrassing hole it in their defenses.

New models from the XPS, Precision and Inspiron families include a powerful root CA certificate called eDellRoot, which puts the machines' owners at risk of identity theft and banking fraud.

The self-signed certificate is bundled with its private key, which is a boon for man-in-the-middle attackers: for example, if an affected Dell connects to a malicious Wi-Fi hotspot, whoever runs that hotspot can use Dell's cert and key to silently decrypt the victims' web traffic. This would reveal their usernames, passwords, session cookies and other sensitive details, when shopping or banking online, or connecting to any other HTTPS-protected website.

Stunningly, the certificate cannot be simply removed: a .DLL plugin included with the root certificate reinstalls the file if it is deleted. One has to delete the .DLL – `Dell.Foundation.Agent.Plugins.eDell.dll` – as well as the eDellRoot certificate.

Dell has posted information [.docx] on how to do this properly, and future machines will not include the dangerous root CA cert. A software update process will run from November 24 that will remove the certificate automatically from machines, we're told.

In a statement to the media, the Texas-based IT titan said:

The recent situation raised is related to an on-the-box support certificate intended to provide a better, faster and easier customer support experience. Unfortunately, the certificate introduced an unintended security vulnerability.

Dell said that it started including the root CA certificate with machines in August, although an Inspiron 15 series laptop we bought in July has an eDellRoot certificate on it.

"We deeply regret that this has happened and are taking steps to address it," added Laura Thomas, Dell's chief blogger.

"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. This certificate is not being used to collect personal customer information.

"It's also important to note that the certificate will not reinstall itself once it is properly removed using the recommended Dell process."

If you've got a new Dell, you can check here to see if you the dodgy root CA cert installed. For everyone, we'll leave you with this nightmare fuel... ®

We found a SCADA system on the Internet using the eDellRoot cert for HTTPS:https://t.co/N5XWQMTuFC #eDellRoot pic.twitter.com/4SoBhcMEL3

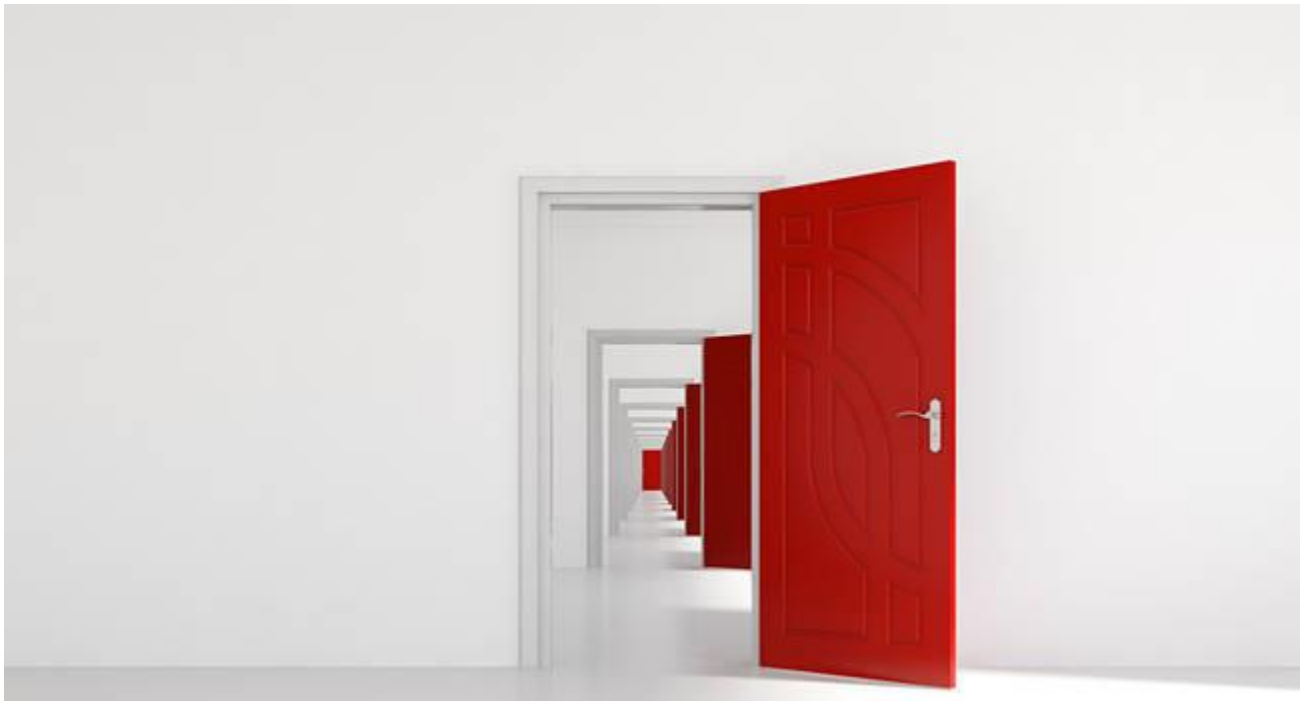
— Duo Labs (@duo_labs) November 24, 2015

Republished for educational purposes.

Security

Second Dell backdoor root cert found

Blackhats, head straight to the airport lounge.



25 Nov 2015 at 05:00, Darren Pauli

A second root certificate has been found in new Dell laptops days after the first backdoor was revealed.

The DSDTestProvider certificate was first discovered by *Laptopmag*. It is installed through Dell System Detect into the Trusted Root Certificate Store on new Windows laptops along with the private key.

Dell has been contacted for comment. The Texas tech titan has called the first certificate gaffe an "unintended security vulnerability" in boilerplate media statements.

Carnegie Mellon University CERT says it allows attackers to create trusted certificates and impersonate sites, launch man-in-the-middle attacks, and passive decryption.

"An attacker can generate certificates signed by the DSDTestProvider CA (Certificate Authority)," CERT bod Brian Gardiner says.

"Systems that trusts the DSDTestProvider CA will trust any certificate issued by the CA.

"An attacker can impersonate web sites and other services, sign software and email messages, and decrypt network traffic and other data. Common attack scenarios include impersonating a web site, performing a MiTM attack to decrypt HTTPS traffic, and installing malicious software."

Punters should move the DSDTestProvider certificate to the untrusted store using Windows certificate manager. They also need to kill `Dell.Foundation.Agent.Plugins.eDell.dll` to stop persistence.

The eDellRoot certificate was found this week in XPS, Precision, and Inspiron laptops.

Security bod Robert Graham ~~recommends~~ says black hats should head straight to the international airport lounge and use the handy certificates and keys to plunder executives' laptops.

"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," Graham says.

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

Security

Dell: How to kill that web security hole we put in your laptops, PCs

Promises to automatically remove root CA cert from machines from Nov 24

24 Nov 2015 at 01:14, Chris Williams

Dell has published a guide on how to remove the web security backdoor it installed in its Windows laptops and desktop PCs.

This confirms what we all know by now – that Dell was selling computers with a rather embarrassing hole it in their defenses.

New models from the XPS, Precision and Inspiron families include a powerful root CA certificate called eDellRoot, which puts the machines' owners at risk of identity theft and banking fraud.

The self-signed certificate is bundled with its private key, which is a boon for man-in-the-middle attackers: for example, if an affected Dell connects to a malicious Wi-Fi hotspot, whoever runs that hotspot can use Dell's cert and key to silently decrypt the victims' web traffic. This would reveal their usernames, passwords, session cookies and other sensitive details, when shopping or banking online, or connecting to any other HTTPS-protected website.

Stunningly, the certificate cannot be simply removed: a .DLL plugin included with the root certificate reinstalls the file if it is deleted. One has to delete the .DLL – `Dell.Foundation.Agent.Plugins.eDell.dll` – as well as the eDellRoot certificate.

Dell has posted information [.docx] on how to do this properly, and future machines will not include the dangerous root CA cert. A software update process will run from November 24 that will remove the certificate automatically from machines, we're told.

In a statement to the media, the Texas-based IT titan said:

The recent situation raised is related to an on-the-box support certificate intended to provide a better, faster and easier customer support experience. Unfortunately, the certificate introduced an unintended security vulnerability.

Dell said that it started including the root CA certificate with machines in August, although an Inspiron 15 series laptop we bought in July has an eDellRoot certificate on it.

"We deeply regret that this has happened and are taking steps to address it," added Laura Thomas, Dell's chief blogger.

"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. This certificate is not being used to collect personal customer information.

"It's also important to note that the certificate will not reinstall itself once it is properly removed using the recommended Dell process."

If you've got a new Dell, you can check here to see if you the dodgy root CA cert installed. For everyone, we'll leave you with this nightmare fuel... ®

We found a SCADA system on the Internet using the eDellRoot cert for HTTPS:https://t.co/N5XWQMTuFC #eDellRoot pic.twitter.com/4SoBhcMEL3

— Duo Labs (@duo_labs) November 24, 2015

Republished for educational purposes.