24 NOV 2015 NEWS

Dell PCs Ship Preloaded with Flawed Certificates

Tara Seals US/North America News Reporter, Infosecurity Magazine

Email Tara

Dell PCs have been shipping to users with certificates that attackers could easily clone to impersonate any HTTPS-protected website, such as online banking and Google.

This issue is similar to the Lenovo Superfish problem uncovered earlier this year. In that case, news that some Lenovo laptop models came with adware pre-installed. The Chinese PC player first tried to head off criticism by claiming the software was designed to "enhance the shopping experience" for customers by presenting them with ads for products similar to ones they'd been searching for. However, it soon came under fire after it emerged that the adware installs its own CA certificate to work, raising the possibility that hackers could use the program to launch man-in-the-middle attacks against users.

In this case, there are two trusted root certificates found on Dell machines, including eDellRoot. Duo Security identified one of the systems in the wild using the eDellRoot for providing web services over HTTPS was a SCADA system.

eDellRoot is shipped with an associated private key, which Duo Security characterizes as an "epic fail."

That's a view that's also echoed by other researchers. "Dell PCs ship with their own certificate authority as root, including their private key for the certificate authority, meaning anyone can impersonate Dell," said Andrew Lewman, VP of data development at Norse, in an emailed comment. "Any enterprise should be reloading their operating systems on delivery and not simply using what comes from the factory by default."

Also, Duo Security said that its research indicates that Dell is intentionally shipping identical private keys in other models as well—and it also found another certificate mishap on a Dell machine—an Atheros Authenticode certificate, which also shipped with Bluetooth software.

In all, this means an attacker could sniff a Dell user's web browsing traffic and manipulate their traffic to deliver malware.

"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, emails, etc.," explained the firm. "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."

To protect themselves, Lewman recommended that 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.

Photo © MR. INTERIOR

Lenovo Claims Superfish Preloads Stopped in January but Fears Persist

Lenovo Releases Superfish Removal Tool

Businesses Using Millions of Flawed Certificates

Let's Encrypt Promises Free Digital Certificates for HTTPS

What's Hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

1. 24 NOV 2015 NEWS
   US Retailers on High Alert After ModPos Malware Warning
2. 23 NOV 2015 NEWS
   GlassRAT Zero-Detection Trojan Targets Chinese Nationals
3. 23 NOV 2015 NEWS
   Porn is Mobile Malware's Favorite Disguise
4. 23 NOV 2015 NEWS
   F&S: Security To Be Biggest ICT Issue in 2016
5. 23 NOV 2015 NEWS
   Russian Cybercrime Gangs Flourish with 1,000 New Employees
6. 23 NOV 2015 NEWS
   Networking Engineer Crowned UK Cybersecurity Champion