Superfish 2.0: Dell Windows Systems Pre-Installed TLS Root CA

Recently shipped Dell systems have been found to include a special Root CA Certificate and private key, "eDellRoot". All systems apparently use the same key and certificate. Using the "secret" key, anybody could create certificates for any domain, and Dell systems with this eDellRoot certificate would trust it. The key is part of "Dell Foundation Services".

To test if your system is affected, see: https://edell.tlsfun.de

To remove the certificate if you are affected:

- stop and disable Dell Foundation Services
- delete the eDellRoot CA (start certmgr.msc, select "Trusted Root Certification Authorities" and "Certificates". Look for eDellRoot)

For details about managing Root CAs see https://technet.microsoft.com/en-us/library/cc754841.aspx

In this case, it is not sufficient to just remove the CA. Dell Foundation Services will reinstall it. This is why you need to disable Dell Foundation Services first, or delete the Dell.Foundation.Agent.Plugins.eDell.dll.

Johannes B. Ullrich, Ph.D.
STI|Twitter|LinkedIn

Reply Subscribe