Dell resellers should urge customers to check if their devices are affected by eDellRoot, a security vulnerability found in an August 2015 Dell software update.

First noticed by programmer Joe Nord, eDellRoot is a trusted root certificate pre-installed in Dell machines. Following a bit of sleuthing Nord discovered eDellRoot is has locally stored private key-- opening a vulnerability for unscruplous hackers, since the key is stored on the computer itself, rather than kept by the issuing authority.

“The same private key was found on multiple machines, meaning that anybody that has access to it can now use it to impersonate the certificate holder [i.e. the PC owner],” Malwarebytes security researcher Jérôme Segura tells Wired. “It made matters worse that the password for that key was easily crackable.”

The incident has been (rightfully) compared to Superfish, the dangerous HTTPS-breaking adware found pre-installed in Lenovo notebooks earlier this year. However, Dell insists eDellRoot "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," and as such was not used to collect private customer information.

The company also provides instructions on how to permanently remove the certificate from affected systems.

The moral of the story? As Dell itself puts it, "in today’s world of ever-increasing cybersecurity

threats, we all need to be vigilant." So do check with your customers if you resell Dell hardware.

Go New Dell Computer Comes with a eDellRoot Trusted Root Certificate

Go Response to Concerns Regarding eDellRoot Certificate

Go Dell Promised Security... Then Delivered a Huge Security Hole (Wired)