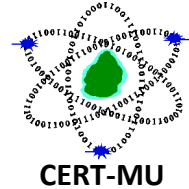


# CERT-MU Security Alert



## Dell computers affected by eDellRoot self-signed root certificate

**Original Issue Date:** November 25, 2015

**Severity Rating:** High

### Affected Systems:

- Inspiron 7000 (laptop and desktop)
- Dell Orchid Touch
- Dell t4034

### Description:

A security issue has been identified in some Dell computers which could be exploited by remote attackers to conduct man-in-the-middle attacks. The security issue lies with a root certificate authority (eDellRoot) which was valid through 2039.

Dell installs a self-signed root certificate authority, eDellRoot, on a number of their computers, along with the private key. The issue here is that the private key has been exposed since it was used across a number of Dell computers. This can allow attackers to perform man-in-the-middle attacks on the affected computers.

Besides man-in-the-middle attacks, the eDellRoot certificate authority and private key can also allow attackers to sign code. This means that attackers can sign malware as if it was from another company, but it will look legitimate to computers with the eDellRoot certificate authority installed. This can also allow attackers to easily masquerade as legitimate software on Dell computers affected by this issue.

Security experts have already detected malware signed with eDellRoot certificate authority.

### Impact:

Man-in-the-middle attacks

### Workarounds:

Dell has provided removal instructions to correct the problem and will be issuing a software update to check for the certificate and remove it, if present.

The removal instruction is available on:

<https://dellupdater.dell.com/Downloads/APP009/eDellRootCertificateRemovalInstructions.pdf>

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: [unsubscribe@cert.ncb.mu](mailto:unsubscribe@cert.ncb.mu)

For more information please contact CERT-MU team on:

**Hotline No:** (+230) 800 2378

**Fax No:** (+230) 208 0119

**Gen. Info:** [contact@cert.ncb.mu](mailto:contact@cert.ncb.mu)

**Incident:** [incident@cert.ncb.mu](mailto:incident@cert.ncb.mu)

**Website:** [www.cert-mu.org.mu](http://www.cert-mu.org.mu)