

[NT] Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0115.html>

From: support@securiteam.com

Date: 08/30/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 30 Aug 2002 11:16:49 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates

SUMMARY

All versions of Windows ship with an ActiveX control known as the Certificate Enrollment Control, the purpose of which is to allow web-based certificate enrollments. The control is used to submit PKCS #10 compliant certificate requests, and upon receiving the requested certificate, stores it in the user's local certificate store.

The control contains a flaw that could enable a web page, through an extremely complex process, to invoke the control in a way that would delete certificates on a user's system. An attacker who successfully exploited the vulnerability could corrupt trusted root certificates, EFS encryption certificates, email-signing certificates, and any other certificates on the system, thereby preventing the user from using these features.

An attack could be carried out through either of two scenarios. The attacker could create a web page that exploits the vulnerability, and host it on a web site in order to attack users who visited the site. The attacker also could send the page as an HTML mail in order to attack the recipient.

Securiteam: [NT] Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates

A new version of the control is available that corrects the vulnerability, and can be installed via the patch. A