

Microsoft released a security patch last week (approximately 28 Aug 2002) to its certificate enrollment control in xenroll.dll. This changes the GUID and some of the behavior of this control. The details can be found in the Knowledge Base article (Q323172) accompanying this security bulletin:

<http://www.microsoft.com/technet/security/bulletin/MS02-048.asp>

This change is not compatible with our Iplanet CMS server.

We propose to change the CMS server to be compatible with this security hotfix. This change would be put into effect on Monday, 09 Sep 2002. We will change the server so that the VBScript it downloads to the client will reference the new GUID (*classid*). We will *not* be replacing the xenroll.dll provided as part of the Iplanet server. Customers will have to apply the Microsoft Hotfix (or some later equivalent patch) in order to use the enrollment page (or use a different browser).

A new customer UI page can be seen here:

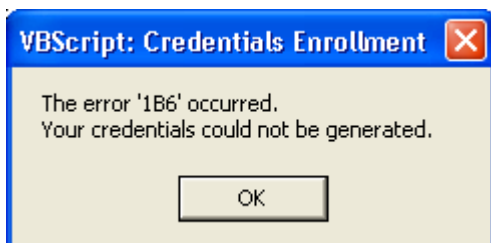
<http://corvette.es.net:1024>

The new xenroll.dll has some behavior changes. See Details.

Details

Iplanet will have to patch the server; but we don't expect this to happen for some time.

This error popup will appear when an unpatched IE submits a CSR to a Patched CMS or a patched IE submits a CSR to an unpatched CMS.

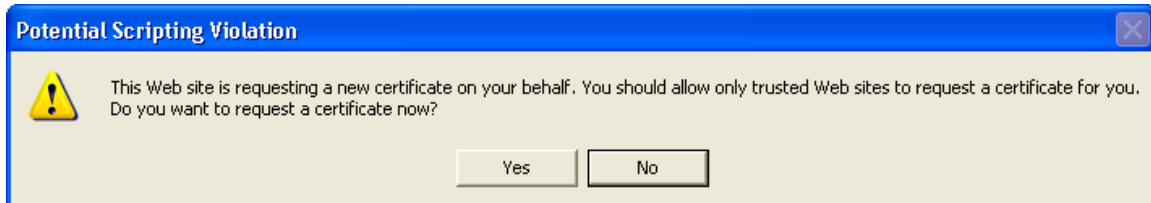


This strange error message won't help anyone.

We experimented with downloading the new xenroll.dll to unpatched clients. This works, but causes a subsequent hotfix installation to be very confusing. The system is left in a state where it is not easy to tell whether the security fix in Q323172 is actually applied. Even if we could redistribute Microsoft's xenroll.dll, which may be allowable, this confusion doesn't seem acceptable. This problem needs to be solved by Iplanet.

The good news about this is we finally have a full, proved understanding of how this dll works. It is very unlikely that anyone has ever downloaded the xenroll.dll from our CMS, as doing so would have caused a download alert to appear. In most modern Windows instances this certificate enrollment interface was already registered and available locally.

Once a customer has applied this hotfix, the Certificate Enrollment DLL behaves differently than before. This new alert pops up when a patched IE submits a CSR to a patched CMS:



Every time a certificate is retrieved (including the CA certificates) this alert appears:

