CERT Advisory CA-2000-08 Inconsistent Warning Messages in Netscape Navigator

Original release date: May 26, 2000
Last Revised: May 27, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Netscape Navigator, up to and including Navigator 4.73, without the Personal Security Manager installed

Overview

A flaw exists in Netscape Navigator that could allow an attacker to masquerade as a legitimate web site if the attacker can compromise the validity of certain DNS information. This is different from the problem reported in CERT Advisory CA-2000-05, but it has a similar impact. This vulnerability was recently discovered by Kevin Fu of of the Massachusetts Institute of Technology and, independently, by Jon Guyer.

If a user visits a web site in which the certificate name does not match the site name and proceeds with the connection despite the warning produced by Netscape, then subsequent connections to any sites that have the same certificate will not result in a warning message.

It should be noted that neither this vulnerability, nor the one described in CERT Advisory CA-2000-05 represent a weakness or vulnerability in SSL. Rather, these problems are a result of the fundamentally insecure nature of the DNS system, combined with an over-reliance on web browsers to do "sanity checking." In both cases, it is (and has been) within the power of the user to validate connections by examining certificates and verifying the certificates against their expectations.

Netscape and other browsers take steps to warn users when the DNS information appears to be suspicious; the browser may not be able to do all the checks necessary to ensure that the user is connecting to the correct location. Therefore, as a general practice, the CERT/CC recommends validating certificates before any sensitive transactions.

I. Description

Digital certificates are small documents used to authenticate and encrypt information transmitted over the Internet. One very common use of digital certificates is to secure electronic commerce transactions through SSL. The kind of certificates used in e-commerce transactions are called X.509 certificates. The X.509 certificates help a web browser and the user ensure that any sensitive information transmitted over the Internet is readable only by the intended recipient. This requires verifying the recipient's identity and encrypting data so that only the recipient can decrypt it.

The "padlock" icon used by Netscape, Internet Explorer, and other browsers is an indication that an SSL-secured transaction has been established to *some one*. It does not necessarily indicate to whom the connection has been established. Netscape and other browsers take steps to warn users when DNS-based information conflicts with the strongly authenticated information contained in the X.509 certificates used in SSL transactions. These warnings are supplemental information to help users decide if they're connecting to whom they think they are connecting. These steps and warnings are designed to protect against attacks on the DNS information.

If you rely solely on the warning dialogs provided by web browsers to determine if the connection is with whom you think it is or if you do not fully understand the implications of the dialogs, then you may be subject to the attacks described in this document and CA-2000-05.

The essence of the problem is this: Within one Netscape session, if a user clicks on "continue" in response to a "hostname does not match name in certificate" error, then that certificate is incorrectly validated for future use in the Netscape session, **regardless** of the hostname or IP address of other servers that use the certificate.

For example, suppose that an attacker constructs a web site named example.com, authenticated by a certificate that does **not** match example.com, and convinces a victim to navigate there. Netscape will present a warning dialog indicating that the site to which the user thinks she's navigating (www.example.com) does not match the information presented in the certificate. If the user does not intend to provide any sensitive information to www.example.com, she may choose to continue with the connection (i.e., she may choose to click "OK" in response to the warning dialog), possibly attributing the warning dialog to a benevolent misconfiguration on the part of example.com or failing to understand the implications of the warning dialog.

Then, within the same session, no warning dialogs will be presented under the following circumstances:

- the attacker co-opts the DNS system in some fashion to cause the DNS name of a legitimate site to resolve to the IP address of a system under the control of the attacker
- the system under the control of the attacker is authenticated using the same certificate as www.example.com, which the user previously accepted in the warning dialog mentioned above
- the victim attempts to connect to the legitimate site (but instead gets directed to the site under the control of the attacker by virtue of the attack on DNS)

This allows the attacker to bypass the ordinary "sanity checking" done by Netscape, and the result is that the user may provide sensitive information to the attacker.

II. Impact

Attackers can trick users into disclosing information (such as credit card numbers, personal data, or other sensitive information) intended for a legitimate web site - if the user has previously accepted a certificate in which the name recorded in the certificate does not match the DNS name of the web site to which the user is connecting.

III. Solution

Check Certificates

The CERT/CC recommends that prior to providing any sensitive information over SSL, you check the name recorded in the certificate to be sure that it matches the name of the site to which you think you are connecting. For example, in Netscape, click on the "padlock" icon to engage the "Security Info" dialog box. Then click on the "View Certificate" button. A dialog box will appear, listing the certificate authority that signed the certificate and the server for which it was issued. If you do not trust the certificate authority or if the name of the server does not match the site to which you think you're connecting, be suspicious.

Validate Certificates Independently

Web browsers come configured to trust a variety of certificate authorities. If you delete the certificates of all the certificate authorities in your browser, then whenever you encounter a new SSL certificate, you will be prompted to validate the certificate yourself. You can do this by validating the fingerprint on the certificate through an alternate means, such as the telephone. That is, the same dialog box mentioned above also lists a fingerprint for the certificate. If you wish to validate the certificate yourself, call the organization for which the certificate was issued and ask them to confirm the fingerprint on the certificate.

Deleting the certificates of the certificate authorities in your browser will cause the browser to prompt you for validation whenever you encounter a new site certificate. This may be inconvenient and cumbersome, but it provides you with greater control over which certificates you accept.

It is also important to note that this sort of verification is only effective if you have an independent means through which to validate the certificate. This sort of validation is called *out-of-band* validation. For example, calling a phone number provided on the *same* web page as the certificate does not provide any additional security.

The CERT/CC encourages all organizations engaging in electronic commerce to train help desk or customer support personnel to answer questions about certificate fingerprints.

Reject certificates that don't match the host name

As a specific defense against this vulnerability, we recommend not accepting certificates that don't match the host name. The most likely cause of a non-matching certificate is a configuration error on the part of the web server administrator. However, a user is unable to distinguish between a benign misconfiguration and a malicious attack. Even if the user does not intend to provide any sensitive information to a site with a non-matching certificate, answering "OK" to this dialog may permit an attacker to successfully carry out the exploit.

Stay up-to-date with patches, workarounds, and certificate management products

Apply a patch from your vendor. Appendix A contains vendor information.

Appendix A Vendor Information

iPlanet

[...] the potential exploit in question can be completely prevented if the user does not click "continue" as stated above. Because of this safety measure, we do not feel an emergency release is necessary. However, we are planning on addressing this in a future release of Communicator, scheduled for release later this year.

Additionally, this flaw was fixed in PSM approximately 6 months before [the initial report of the vulnerability].

The CERT Coordination Center thanks Kevin Fu of MIT and Jon Guyer for initially discovering and reporting this vulnerability, and their help in constructing this advisory.

Shawn Hernan was the primary author of this document.

Revision History

```
May 26, 2000: initial release
May 27, 2000: clarified information from iPlanet
```