

[NT] Certificate Validation Flaw Could Enable Identity Spoofing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0024.html>

From: support@securiteam.com

Date: 09/06/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 6 Sep 2002 19:29:52 +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.

Certificate Validation Flaw Could Enable Identity Spoofing

SUMMARY

The IETF Profile of the X.509 certificate standard defines several optional fields that can be included in a digital certificate. One of these is the Basic Constraints field, which indicates the maximum allowable length of the certificate's chain and whether the certificate is a Certificate Authority or an end-entity certificate. However, the APIs within CryptoAPI that construct and validate certificate chains (CertGetCertificateChain(), CertVerifyCertificateChainPolicy(), and WinVerifyTrust()) do not check the Basic Constraints field. The same flaw, unrelated to CryptoAPI, is also present in several Microsoft products for Macintosh.

The vulnerability could enable an attacker who had a valid end-entity certificate to issue a subordinate certificate that, although bogus, would nevertheless pass validation. Because CryptoAPI is used by a wide range of applications, this could enable a variety of identity spoofing attacks. These are discussed in detail in the FAQ, but could include:

- * Setting up a web site that poses as a different web site, and "proving" its identity by establishing an SSL session as the legitimate web site.

- * Sending emails signed using a digital certificate that purportedly

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

belongs to a different user.

- * Spoofing certificate-based authentication systems to gain entry as a highly privileged user.

- * Digitally signing malware using an Authenticode certificate that claims to have been issued to a company users might trust.

DETAILS

Affected Software:

- * Microsoft Windows 98
- * Microsoft Windows 98 Second Edition
- * Microsoft Windows Me
- * Microsoft Windows NT® 4.0
- * Microsoft Windows NT 4.0, Terminal Server Edition
- * Microsoft Windows 2000
- * Microsoft Windows XP
- * Microsoft Office for Mac
- * Microsoft Internet Explorer for Mac
- * Microsoft Outlook Express for Mac

Mitigating factors:

Overall:

- * The user could always manually check a certificate chain, and might notice in the case of a spoofed chain that there was an unfamiliar intermediate CA.

- * Unless the attacker's digital certificate were issued by a CA in the user's trust list, the certificate would generate a warning when validated.

- * The attacker could only spoof certificates of the same type as the one he or she possessed. In the case where the attacker attempted an attack using a high-value certificate such as Authenticode certificates, this would necessitate obtaining a legitimate certificate of the same type – which could require the attacker to prove his or her identity or entitlement to the issuing CA.

Web Site Spoofing:

- * The vulnerability provides no way for the attacker to cause the user to visit the attacker's web site. The attacker would need to redirect the user to a site under the attacker's control using a method such as DNS poisoning. As discussed in the FAQ, this is extremely difficult to carry out in practice.

- * The vulnerability could not be used to extract information from the user's computer. The vulnerability could only be used by an attacker as a means of convincing a user that he or she has reached a trusted site, in the hope of persuading the user to voluntarily provide sensitive data.

Email Signing:

- * The "from" address on the spoofed mail would need to match the one specified in the certificate, giving rise to either of two scenarios if a recipient replied to the mail. In the case where the "from" and "reply-to" fields matched, replies would be sent to victim of the attack rather than

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

the attacker. In the case where the fields did not match, replies would obviously be addressed to someone other than ostensible sender. Either case could be a tip-off that an attack was underway.

Certificate-based Authentication:

* In most cases where certificates are used for user authentication, additional information contained within the certificate is necessary to complete the authentication. The type and format of such data typically varies with every installation, and as a result significant insider information would likely be required for a successful attack.

Authenticode Spoofing:

* To the best of Microsoft's knowledge, such an attack could not be carried out using any commercial CA's Authenticode certificates. These certificates contain policy information that causes the Basic Constraints field to be correctly evaluated, and none allows end-entity certificates to act as CAs.

* Even if an attack were successfully carried out using an Authenticode certificate that had been issued by a corporate PKI, it wouldn't be possible to avoid warning messages, as trust in Authenticode is brokered on a per-certificate, not per-name, basis.

Patch availability:

Download locations for this patch

* Microsoft Windows 98:

To be released shortly

* Windows 98 Second Edition:

To be released shortly

* Windows Me:

To be released shortly

* Windows NT 4.0:

<<http://www.microsoft.com/ntserver/nts/downloads/critical/q328145/default.asp>>

<http://www.microsoft.com/ntserver/nts/downloads/critical/q328145/default.asp>

* Windows NT 4.0 Terminal Server Edition:

<<http://www.microsoft.com/ntserver/terminalserver/downloads/critical/q328145/default.asp>>

<http://www.microsoft.com/ntserver/terminalserver/downloads/critical/q328145/default.asp>

* Windows 2000:

To be released shortly

* Windows XP:

<<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=42562>>

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=42562>

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

* Windows XP 64 bit Edition:

<<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=42558>>
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=42558>

* Microsoft Office v.X for Mac:

To be released shortly

* Microsoft Office 2001 for Mac:

To be released shortly

* Microsoft Office 98 for the Macintosh:

To be released shortly

* Microsoft Internet Explorer for Mac (for OS 8.1 to 9.x):

To be released shortly

* Microsoft Internet Explorer for Mac (for OS X):

To be released shortly

* Microsoft Outlook Express 5.0.5 for Mac:

To be released shortly

The patch availability section lists a number of products, but patches are not available for all of them. Why not?

Normally, Microsoft does release the patches for all affected product simultaneously, in order to provide a complete solution. However, exploit code for this issue has already been posted, and we are therefore releasing the patches as they become available, in order to allow customers to begin protecting their systems as quickly as possible.

What is the scope of the vulnerability?

This vulnerability could enable an attacker to construct a digital certificate that, although bogus, would nevertheless be accepted as bona fide. Digital certificates are used for a variety of security-related purposes – for instance, users use them to confirm those web sites' identities; to verify who the sender of an email was; whether it is safe to run particular programs, and other purposes – and the ability to forge a seemingly valid certificate could allow a variety of attacks.

In many cases, the specific policies followed by the companies that issue digital certificates mitigate the risk posed by the vulnerability. These policies could make it difficult or impossible to successfully exploit the vulnerability, and in some cases could make it easier to determine who carried out a particular attack. In addition, it is worth noting that it would always be possible for a user to examine a digital certificate and see telltale signs of an attempt to exploit the vulnerability.

What causes the vulnerability?

The vulnerability occurs because of flaws in the way the affected products evaluate the Basic Constraints field when validating a digital certificate. These flaws could enable an attacker to act as a Certificate

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

Authority and create subordinate certificates with any desired information, which the affected products would accept as valid.

What is a digital certificate?

Digital certificates are a familiar fixture within public-key cryptography. In public-key cryptography, there are two keys: the private key, which must be kept secret, and the public key, which is intended to be shared with the world. In order for the public key to be shared effectively, there needs to be a way to learn whose it is, how it can be used, and to verify that the information is bona fide. Digital certificates provide a way to do this.

A digital certificate combines a public key with information about it – who owns it, what purposes it can be used for, when it expires, and so forth. When a user needs a digital certificate, he or she gets it from an organization known as a Certificate Authority (CA). The CA not only creates the certificate, it also digitally signs it, thereby vouching for the information in it and preventing it from being modified without detection.

What are digital certificates used for?

Here is a sampling of some applications that use digital certificates:

- * Web sessions. Web sites frequently use the Secure Sockets Layer protocol, which allows a web site to prove to visitors that it is the one it purports to be, and to provide encryption for the resulting web session.
- * Email. Many email clients support S/MIME, a protocol that uses digital certificates to prove the origination point and authenticity of an email.
- * Code signing. Microsoft platforms support Authenticode, a technology that lets software developers digitally sign their programs in order to prove their authorship and to show that the programs have not been modified.
- * Networking sessions. Many companies use IPSEC to protect network sessions by encrypting them and enabling the participants to know with certainty who they are communicating with.

How is the functionality implemented to support digital certificates?

Applications implement support for digital certificates in either of two ways. Those that run under Windows typically make use of CryptoAPI, a set of functions built into Windows that provide support for encryption, decryption, digital certificate handling, and other tasks. Those that run under other operating systems typically must implement cryptographic functions locally – that is, within the applications themselves.

Does the vulnerability in this case lie in CryptoAPI or in local implementations within particular products?

Both. The CryptoAPI implementation is affected by the vulnerability, and

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

therefore affects all applications – whether written by Microsoft or a third party – that use it. However, several Microsoft applications that run on the Macintosh (and therefore provide their own cryptographic implementations) contain the same vulnerability.

What is wrong with how digital certificates are validated in the affected products?

The vulnerability results because the affected products do not check a particular field – known as Basic Constraints – when validating a digital certificate. As we discussed above, one of the purposes of a digital certificate is to allow the CA that issued it to regulate how it can be used. The Basic Constraints field is one way through which this is done.

The Basic Constraints field allows the CA to indicate two important pieces of information: whether the certificate is authorized to act as a CA in its own right (and thereby issue additional, subordinate certificates), and how long the resulting chain of certificates can be. The affected products do not check this field and therefore do not apply any of the constraints that it may indicate.

Why does this pose a security vulnerability?

As we discussed above, when a CA issues a digital certificate, it vouches for the authenticity of the certificate and the identity of the owner. The flaw poses a security vulnerability because, in essence, it could allow an attacker who has been issued a digital certificate to successfully claim that the CA has delegated to him the ability to issue additional certificates. The attacker's assertions about the validity of those certificates would carry the same force as if they had been made by the CA itself.

What would this vulnerability enable an attacker to do?

The vulnerability could enable an attacker to create bogus a digital certificate that would nevertheless pass validation. Depending on the usage, this could enable a variety of attacks, such as:

- * Creating a web site that could successfully pose as a different web site, in the hope that visitors would provide sensitive information to it.
- * Sending an email whose digital signature would attest that it was sent by someone other than the actual sender.
- * Posing as another user by providing a bogus digital certificate as authentication.
- * Digitally signing a dangerous program in the guise of a trustworthy user or company, in order to convince a user that it was safe to run it.

It is important to understand that each of these scenarios would be subject to operational barriers of varying degrees. We will discuss each scenario in detail below, but it is worth listing three obstacles that would be common to all of these scenarios.

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

* The attacker's digital certificate would need to be issued by a CA that the user trusted. The attacker's point in exploiting the vulnerability would be to create a bogus certificate that generated no warning messages, but if the CA that issued the attacker's certificate were not trusted, that fact in itself would generate a warning.

* The bogus certificate would be limited to the same usage as the attacker's. This means that, in order to create a bogus SSL server certificate, the attacker would need a valid SSL server certificate; in order to create a bogus Authenticode certificate, the attacker would need a valid Authenticode certificate, and so forth. In some cases, obtaining a valid certificate could require that the attacker provide proof of identity that could later be used by law enforcement.

* The user could always determine the truth. Every Microsoft application that uses digital certificates provides a way to view the certificate. A user who did so might notice that the certificate chain was unusual, in that the issuer of the certificate was an unfamiliar name and did not appear to be affiliated with the CA.

How might an attacker use the vulnerability to spoof a trusted web site? The attacker would likely select an e-commerce site that users would be likely to trust, set up a web site that purported to be the legitimate e-commerce site, then create a bogus SSL server certificate bolstering that claim. If a user visited the attacker's site, the certificate would allow it to set up a valid SSL session, "confirming" that it was indeed the legitimate e-commerce site. The user might then choose to provide sensitive information such as credit card numbers to the attacker's site.

The chief obstacle this scenario would pose is that the vulnerability provides no way to make the user actually arrive at the attacker's site, let alone in the belief that it is a different site. Doing this would likely require that the attacker be able to modify the Internet infrastructure that the user transited, via a technique such as DNS cache poisoning. However, such techniques are difficult, temporary, and generally require favorable network topology.

How might an attacker use the vulnerability to spoof digitally signed emails?

The attacker would create a bogus email-signing certificate that purportedly belonged to a different user, then use it to digitally sign an email. The recipient might conclude, based on the signature, that the mail was valid.

The primary problem with this scenario is that, in order for the signature to be validated, the "from" address on the email would need to match the one cited on the certificate. That is, an attacker who wanted to sign mail as Bob would need to create a certificate with Bob's email address on it, and use Bob's address as the "from" address on the email. In most cases, replying to the mail would cause it to be delivered to Bob – not the attacker – and Bob would know that someone was spoofing his signature. The

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

attacker could manipulate the mail fields so that replies would not be sent to Bob, but that in itself would be a tip-off that something was afoot. In either case, it would be relatively simple for the recipient to provide Bob with a copy of the attacker's bogus certificate, which Bob could then have revoked or turn over to law enforcement.

How might an attacker use the vulnerability to spoof certificate-based authentication?

This scenario would apply to atypical cases, such as one in which mutually authenticating SSL sessions are used to broker access to network resources. To carry out an attack against such a system, the attacker would generate a bogus certificate in the name of another user – presumably, an administrator or other privileged user – then use the certificate to authenticate as that user, thereby gaining the other user's privileges.

There are two chief obstacles to this attack. First, scenarios like this one typically are found within corporate networks where public key infrastructures have been deployed. In such a case, the attacker could not simply buy a certificate from a commercial CA. Instead, he or she would need to obtain one from the company's local CA, which likely would require the attacker to already be a legitimate network user. Second, systems such as these typically arbitrate user privileges using data stored by the CA within the certificate. Determining the right data, and the right format, could require significant insider knowledge.

How might an attacker use the vulnerability to spoof an Authenticode signature?

To describe just one scenario, the attacker might create an ActiveX control that performs some malicious task, then create an Authenticode digital certificate purporting to belong to a widely trusted company. After using the bogus certificate to digitally sign the control, the attacker could host the control on a web site that he or she controlled, and attempt to run it whenever a user visited the site.

The problem for the attacker in this scenario is that, to the best of Microsoft's knowledge, no commercial CA's Authenticode certificates could be used in such an attack. The reason is that these CAs include policy information within their certificates, the effect of which is to cause CryptoAPI to re-examine – and correctly process – the Basic Constraints field. In every case, the Basic Constraints information within these certificates disallows using them to issue additional certificates. As a result, this scenario would likely be limited to cases in which a company had deployed a public key infrastructure, issued Authenticode certificates that are not as well formed as those of the commercial CAs, and had issued one to the attacker.

Even if there were a commercial CA that did issue certificates suitable for use in such an attack, the user would still see a warning message. Internet Explorer brokers trust on a certificate-by-certificate basis, not on a name-by-name basis. That is, if two certificates had exactly the same

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

name, and the user agreed to trust the first one, Internet Explorer would still generate a warning when the second certificate was encountered.

I am running Windows. Do I need to apply a patch for every application I am running?

No. You just need to apply the patch for the version of Windows you are using. Applying the patch eliminates the vulnerability in CryptoAPI, thereby also making safe any applications that use it.

I am running several of the Microsoft products for Macintosh that you listed above. Do I need to apply a patch for each one?

Yes. Macintosh does not supply a corollary to CryptoAPI, so every application must implement its own cryptography. Consequently, there is a separate patch for each of the Microsoft products for Macintosh listed in the Affected Products listing.

I am a developer, and one of my products uses CryptoAPI. Do I need to do anything?

No. When the patch is applied to a system, it eliminates the problem in CryptoAPI itself, thereby also eliminating the problem in any applications that rely upon it for cryptographic services.

How does the patch address the vulnerability?

The patch ensures that intermediate certificates are not treated as a certificate authority unless the Basic Constraint extension is present with the value of CA set to TRUE. Additionally, the patch ensures that if a KeyUsage extension is present in a certificate purposed to be a certificate authority, it must contain a value for keyCertSign which defines (or restricts) the usage of the key contained in the certificate.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_35964_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>
Microsoft Product Security.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

Securiteam: [NT] Certificate Validation Flaw Could Enable Identity Spoofing

- **Previous message:** support@securiteam.com: "[\[NEWS\] Multiple Remote Vulnerabilities in Polycom Videoconferencing Products](#)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)