IETF X.509 SSL Certificate Signature Collision Vulnerability

< Previous Reference] [Full View] [Next Reference >
[Sign In to Submit Updates] [User Comment Board (0)] [View Policy] [Help]

CVE #:

CVE-2004-2761

Release Date:

December 30, 2008

Vulnerable OS:

Any

Vulnerable Application:

X.509 Certificates

Risk Type:

Unauthorized Access

Summary:

X.509 SSL Certificates using the SHA-1 or MD5 (or weaker MD2/MD4) algorithms may be affected by a vulnerability that can weaken security.

Info:

A vulnerability exists in X.509 certificates which, when signed via MD5, may allow for phishing attacks. Similar vulnerabilities now affect SHA-1 certificates as well.

MD5 certificates have long been deprecated. SHA-1 will be deprecated by most vendors by the end of 2015.

The flaw is specific to weaknesses in the SHA-1 or MD5 algorithm used to sign X.509 certificates. It is possible for a potential attacker to generate multiple pairs of certificates, which share like SHA-1/MD5 signatures. Typical exploration would allow the attacker to impersonate a legitimate website.

Internet Engineering Task Force (IETF) is the standards body for X.509 SSL certification.

General Fix:

This finding may appear on any service that uses an SSL certificate and is not limited to a specific server type or application.

See references or contact the vendor for appropriate patch information. Typically, this problem is associated with NSS libraries or FireFox packages, among other applications. In many cases, this will require obtaining a new certificate for the service (generally HTTPS).

When obtaining a new certificate, make sure an alternative hashing method is utilized to sign them (ex: SHA-256, SHA-512). Also be sure any old certificates are removed.

There is a simple manual method of verifying the certificate details for an offending server. Using a browser, visit the server, typically on port 443/HTTPS. In general, this can simply be done by visiting https://<IP ADDRESS>:<port>/. Most browsers will provide a clickable button to view the certificate information.

In Internet Explorer 8, there is a padlock to the right of the address bar. Clicking it and then "View certificates" brings up a window with a details tab containing the encryption algorithm and date information.

Firefox 3 has a colored area on the left of the address bar containing the domain name that can be clicked. Choosing "More Information" followed by "View Certificate" brings up a similar details window.

Google Chrome is similar to IE8, using a padlock icon on the right of the address bar which can be clicked. Choosing "Certificate information" brings up the same window that IE8 uses.

MSSQL server owners unaware of a certificate in use may be affected by the default certificate described here: http://support2.microsoft.com/kb/2007728 Owners are advised to install a valid, non-default certificate, or disable encryption, depending on the circumstances.

OS Specific Fixes:

Linux

References:

BugTraq

SecurityFocus BID 11849
SecurityFocus BID 33065

CERT

CERT Vulnerability Note VU#836068

Cisco

Cisco Security Response cisco-sr-20090115-md5

Deprecated Refs

Md5WeakSecurity (69071)
X.509 Certificate MD5 Signature Collision Vulnerability (69620)

SSL Certificate Signed using Weak Hashing Algorithm (116218)
MD5-based Signature in TLS/SSL Server X.509 Certificate (179777)

Foundstone

Faultline ID 6360

ISS

ISS vulnerability ID 106907

Microsoft

Microsoft Security Advisory (961509)

Nessus

Plugin ID 35291

OAR

None Mapped

OSVDB

OSVDB ID 45106
OSVDB ID 45108
OSVDB ID 45127

Other

Chosen-prefix Collisions for MD5 and Applications
http://blogs.technet.com/swi/archive/2008/12/30/information-regarding-md5-collisions-problem.aspx
http://www.microsoft.com/technet/security/advisory/961509.mspx

Qualys

Qualys ID 42012

Rapid7

NeXpose Vulnerability tls-server-cert-sig-alg-md5

Secunia

Secunia Advisory SA34446

Ubuntu

Ubuntu Security Notice USN-740-1

XForce

XForce md5-weak-security (47737)