

GreCom Application Service Provider B.V.

Confidential Information

The following report contains confidential information. Do not distribute, email, fax or transfer via any electric mechanism unless it has been approved by your organization's security policy. All copies and backups of this document should be maintained on protected storage at all times. Do not share any of the information contained within this report with anyone unless you confirm they are authorized to view the information.


Disclaimer

This, or any other, vulnerability audit cannot and does not guarantee security. McAfee/PathDefender makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that McAfee/PathDefender shall be held harmless in any event. McAfee/PathDefender makes this information available solely under its Terms of Service Agreement published at www.mcafeesecure.com.

Report Overview

Customer Name	GreCom Application Service Provider B.V.
Date Generated	2014-11-26 23:46
Targets	1
Open Ports	2
Information	1
Vulnerabilities	2

Target Summary

	Target	Last Scan	Open Ports	Vulnerabilities
	uk-fh.risksynccloud.com	2014-11-26 17:59	2	3




Summary

Hostname	uk-fh.risksynccloud.com
Name	none
Tags	none
Last Scan	2014-11-26 17:59

Open Ports

Port	Service
80/tcp	http
443/tcp	http over ssl

Vulnerability Summary

Severity	Name
	SSL Certificate - Subject Common Name Does Not Match Server FQDN
	Default Web Page
	Apache Web Server ETag Header Information Disclosure Weakness

SSL Certificate - Subject Common Name Does Not Match Server FQDN

Severity



Date Found

2014-11-26 17:59

Target

uk-fh.risksynccloud.com

First Found

2014-11-26 17:59

Category

General remote services

Description

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

Consequence

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

Solution

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

Detail Output

Certificate #0 CN=*.patientsafety.com,OU=Domain_Control_Validated_-_RapidSSL(R),
OU=See_www.rapidssl.com/resources/cps_(c)14,OU=GT72700253 (*.patientsafety.com) doesn't resolve (patientsafety.com) and IP
(134.0.76.70) don't match (*.patientsafety.com) doesn't resolve

Default Web Page

Severity			
Date Found	2014-11-26 17:59	Target	uk-fh.risksynccloud.com
First Found	2014-11-26 17:59	Category	CGI

Description

The Result section displays the default Web page for the Web server.

Consequence

None


Solution

None

Detail Output

HTTP/1.1 302 Found Date: Thu, 27 Nov 2014 01:18:31 GMT Server: Apache Location: https://lb-uk-fh.risksynccloud.com Content-Length: 0 Connection: close Content-Type: text/html

Apache Web Server ETag Header Information Disclosure Weakness

Severity		Target	uk-fh.risksynccloud.com
Date Found	2014-11-26 17:59	Category	Web server
First Found	2014-11-26 17:59		

Description

The Apache HTTP Server is a popular, open-source HTTP server for multiple platforms, including Windows, Unix, and Linux.

A cache management feature for Apache makes use of an entity tag (ETag) header. When this option is enabled and a request is made for a document relating to a file, an ETag response header is returned containing various file attributes for caching purposes. ETag information allows subsequent file requests to contain specific information, such as the file's inode number.

A weakness has been found in the generation of ETag headers under certain configurations implementing the FileETag directive. Among the file attributes included in the header is the file inode number that is returned to a client.

Affected Versions:

By default, all Versions of Apache are vulnerable.

In Apache Versions 1.3.22 and earlier, it's not possible to disable inodes in in ETag headers to mitigate this vulnerability, so Apache Version 1.3.22 and earlier are vulnerable at all times.

Apache Version 1.3.23 and later have a setting that can be modified to remove the inode info from the ETag Headers to mitigate this vulnerability. Apache Versions \geq 1.3.23 allow the user to configure what goes into ETag. However, if the user does not configure Apache to not include inode in ETag, the Web server can still be vulnerable even if Apache \geq 1.3.23 is being used.

Consequence

This vulnerability poses a security risk, as the disclosure of inode information may aid in launching attacks against other network-based services. For instance, NFS uses inode numbers to generate file handles.

Solution

Workaround:

For Apache 1.3.22 and earlier:

There is no patch or remediation available for Apache Versions 1.3.22 and earlier since it's not possible to disable inodes in in ETag headers. Customers running versions of Apache \leq 1.3.22 will need to upgrade to a later version and then apply the settings listed below (see Apache Version 1.3.23 and later), as versions of Apache 1.3.22 and earlier do not have the ability to configure these setting.

For Apache 1.3.23 and later: In Apache Version [1.3.23](#) and later, it's possible to configure the FileETag directive to generate ETag headers without inode information, which mitigates this vulnerability.

To do so, include "FileETag -INode" in the Apache server configuration file for a specific subdirectory.

In order to fix this vulnerability globally, for the Web server, use the option "FileETag None". Use the option "FileETag MTime Size" if you just want to remove the Inode information.

OpenBSD:

OpenBSD has released a [patch](#) that fixes this vulnerability. After installing the patch, inode numbers returned from the server are encoded using a private hash to avoid the release of sensitive information.

Detail Output

```
"8045a-1a-4fc18feac5068"
```

Severity Level

Vulnerability



Minimal

Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.



Medium

Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.



Serious

Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.



Critical

Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.



Urgent

Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information



Minimal

Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.



Medium

Intruders may be able to determine the operating system running on the host, and view banner versions.



Serious

Intruders may be able to detect highly sensitive data, such as global system user lists.