McAfee SECURE

Security Report
2015-02-11

GreCom Application Service Provider B.V.

Report Overview

Customer Name	GreCom Application Service Provider B.V.
Date Generated	2015-02-11 23:40
Targets	1
Open Ports	2
Information	1
Vulnerabilities	1

Target Summary

	Target	Last Scan	Open Ports	Vulnerabilities
	uk-fh.risksynccloud.com	2015-02-11 09:15	2	2

uk-fh.risksynccloud.com

Summary

Hostname	uk-fh.risksynccloud.com
Name	none
Tags	none
Last Scan	2015-02-11 09:15

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

SSL Certificate - Subject Common Name Does Not Match Server FQDN

Severity			
Date Found	2015-02-11 09:15	**Target**	uk-fh.risksyncccloud.com
First Found	2015-01-31 00:48	**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	2015-02-11 09:15	**Target**	uk-fh.risksynccloud.com
First Found	2015-01-31 00:48	**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: Wed, 11 Feb 2015 16:37:19 GMT Server: Apache Location: https://lb-uk-fh.risksynccloud.com Content-Length: 0 Connection: close Content-Type: text/html

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.