COPA AIRLINES OPERATIONS & INTELLIGENCE TECHNICAL CYBER SECURITY REPORT

Copa Airlines

May 2018

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com

www.glesec.com

Table of Contents

Table of Contents 2
About This Report 3
Confidentiality 3
Managed Vulnerability Service 4
Description by Host 5
Vulnerabilities found by severity 7
Medium Risk Level Vulnerabilities 7
Low Risk Level Vulnerabilities 8
Whole Compiled Recommendations 16

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

About This Report

This report is a companion to the Monthly Operations & Intelligence Executive Report. The purpose of this document is to provide Technical and Tactical level information, detail and recommendations to the extent that can be summarized. GLESEC processes significant amount of data and not all can be presented in a detail report format. For more information you can review the dashboards of the GMP or if necessary contact us at the GLESEC Operation Centers (GOC).

Confidentiality

GLESEC considers the confidentiality of client's information as a trade secret. The information in this context is classified as:

- Client name and contact information
- System architecture, configuration, access methods and access control
- Security content

All the above information is kept secure to the extent in which GLESEC secures its own confidential information.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Managed Vulnerability Service (MSS-VM)

The Managed Vulnerability Service (MSS-VM) enables organizations to minimize the risk of vulnerabilities by quickly discovering weaknesses, measuring the potential risk and exposure, reporting, providing remediation information necessary to mitigate those risks on an on-going basis and facilitating reporting and compliance with regulations and best practices.

In the address range given by Copa Airlines, we have found a total of 8 hosts, of which 8 are vulnerable. These vulnerabilities are divided in the following severities as shown in the following table. Additionally you can notice the Risk Value score of your organization according to our metrics.

Total IP's Scanned	IP's Vulnerable
8	8

Risk Distribution				
Critical	High	Medium	Low	Total
0	1	21	6	28

According to the metrics:

RV= 0.477083333

The following values are to clarify RV:
RV=1 Points to every IP address in the infrastructure that are susceptible to attacks
RV=0 Points to no IP address in the infrastructure aret susceptible to attacks
RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

All the vulnerabilities found in your organization belong to the following categories:

Category	Critical	High	Medium	Low	Total
General		0	15	3	18
Web Servers		0	4	3	7
CGI abuses		1	0	0	1
Misc.		0	1	0	1
Service detection		0	1	0	1

- General
- Web servers
- Services detection

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

- Misc
- Windows

Additional details about these vulnerabilities are presented in the Vulnerabilities found in Copa Airlines by severity section of the MSS-VM **on page 7.**

Overall the vulnerabilities for Copa Airlines this period have been 1 high, 21 medium and 6 low risk. The vulnerability the high risk is relation with CGI Generic SQL Injection (blind), followed the vulnerabilities have already been reported in previous months. Here are some examples of the most relevant ones: SSL Medium Strength Cipher Suites Supported, SSL Certificate Cannot Be Trusted, SSL Certificate Expiry, SSL RC4 Cipher Suites Supported (Bar Mitzvah), and SSL Certificate Signed Using Weak Hashing Algorithm. The ideal scenario would be for all of these to be hardened, more information about these can be found in the intelligence section for the MSS-VM.

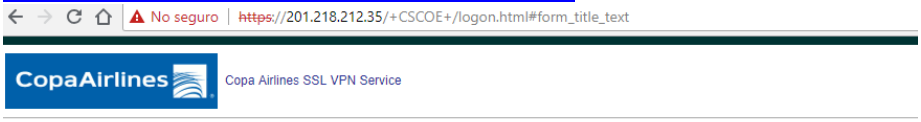
The port considered most vulnerable for this period were 443 (HTTPS) followed 80 (HTTP), 123 (NTP), this is because many vulnerabilities were found which are related to the services listening on them and categorized as medium and low risk.

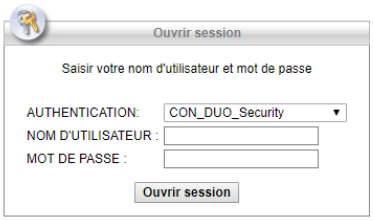
Description by Host

201.218.212.35 (https://201.218.212.35/+CSCOE+/logon.html#form_title_text)
200.46.240.137(https://200.46.240.137/wtouch/wtouch.exe/index?MAC=0&VER=1)
201.218.212.9 (https://201.218.212.9/+CSCOE+/logon.html**)** and other.

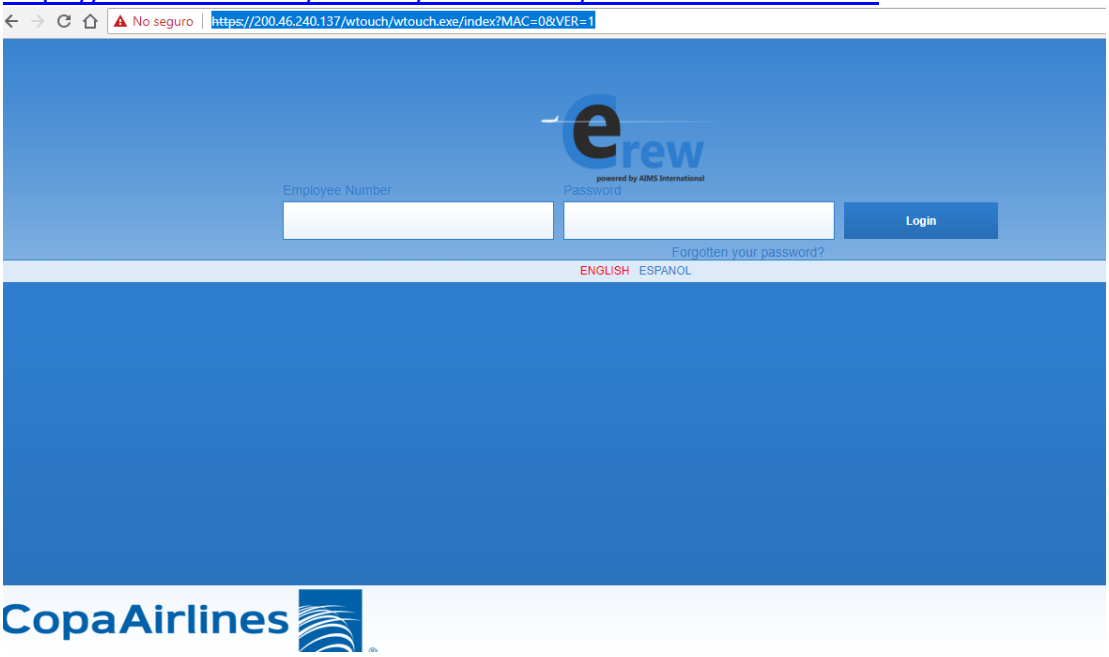
Several vulnerabilities found on this host are stated here:
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported, SSL Self-Signed Certificate, SSL Version 2 and 3 Protocol Detection, SSL Weak Cipher Suites Supported,SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

https://201.218.212.9/+CSCOE+/logon.html

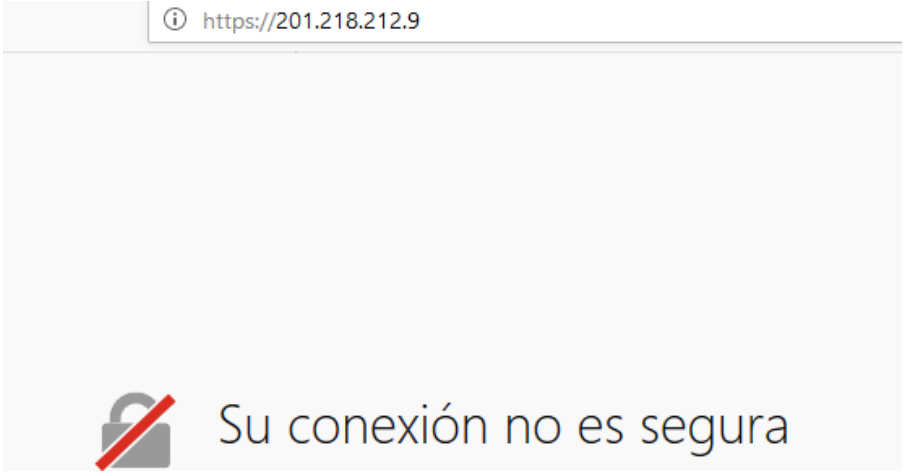




https://200.46.240.137/wtouch/wtouch.exe/index?MAC=0&VER=1



https://201.218.212.9/



Vulnerabilities by severity

The following section will describe in detail each vulnerability found according to their severity.

High Risk Level Vulnerabilities

CGI Generic SQL Injection (blind)

Description
By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, GLESEC was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.
Note that this script is experimental and may be prone to false positives.

Solution
Modify the affected CGI scripts so that they properly escape arguments.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Affected Systems

80 / tcp / possible_wls ec2-52-72-43-239.compute-1.amazonaws.com
443 / tcp / possible_wls ec2-52-72-43-239.compute-1.amazonaws.com

Output

The GET HTTP method GLESEC, found that

```
+ The following resources may be vulnerable to blind SQL injection :

+ The 'nickname' parameter of the /examples/servlets/chat/chat CGI :

/examples/servlets/chat/chat?action=login&nickname='||'login&nickname=

-------- output --------
HTTP/1.1 302 Found
-------- vs --------
HTTP/1.1 400 Bad Request
------------------------

/examples/servlets/chat/chat?action=login&nickname='||'login&nickname= {
2}

-------- output --------
HTTP/1.1 302 Found
-------- vs --------
HTTP/1.1 400 Bad Request
------------------------

+ The 'j_username' parameter of the /examples/jsp/security/j_security_check CGI :

/examples/jsp/security/j_security_check?j_password=&j_username=420239'||
'&j_username=420239

-------- output --------
HTTP/1.1 200 OK
-------- vs --------
HTTP/1.1 400 Bad Request
------------------------

/examples/jsp/security/j_security_check?j_password=&j_username=420239'||
'&j_username=420239 {2}

-------- output --------
HTTP/1.1 200 OK
-------- vs --------
HTTP/1.1 400 Bad Request
------------------------
```


Medium Risk Level Vulnerabilities

Web Application Potentially Vulnerable to Clickjacking

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which

an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Solution
Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Affected Systems

80 / tcp / possible_wls	ec2-52-72-43-239.compute-1.amazonaws.com
443 / tcp / possible_wls	200.46.240.137

Output

```
The following pages do not use a clickjacking mitigation response header and contain a
clickable event :

  - https://200.46.240.137/
```

Apache Tomcat Default Files

Description
The default error page, default index page, example JSPs, and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

Solution
Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

Affected Systems

8080 / tcp / possible_wls	ec2-52-72-43-239.compute-1.amazonaws.com
80 / tcp / possible_wls	ec2-52-72-43-239.compute-1.amazonaws.com
443 / tcp / possible_wls	ec2-52-72-43-239.compute-1.amazonaws.com

Output

```
The following default files were fou

/index.html
/docs/
/examples/servlets/index.html
/examples/jsp/index.html
/examples/websocket/index.xhtml
```

F5 BIG-IP Cookie Remote Information Disclosure

Description
The remote host appears to be an F5 BIG-IP load balancer. The load balancer encodes the IP address of the actual web server that it is acting on behalf of within a cookie. Additionally, information after 'BIGipServer' is configured by the user and may be the logical name of the device. These values may disclose sensitive information, such as internal IP addresses and names.

Affected Systems

443 / tcp / possible_wls	200.46.240.137

Output

```
Cookie       : BIGipServer~AIMS~crew.copa.com.pa=2909608620.47873.0000
IP           : 172.26.109.173
Port         : 443
```

Network Time Protocol (NTP) Mode 6 Scanner

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

Solution

Restrict NTP mode 6 queries.

Affected Systems

123 / udp / ntp 200.46.241.161

Output

```
  host by sending an NTP mode 6 query :

'version="4", processor="unknown", system="UNIX", leap=3, stratum=16,
precision=-24, rootdelay=0.000, rootdispersion=271579.829, peer=0,
refid=INIT, reftime=0xDDA4C5EE.4A0D423A, poll=6,
clock=0xDEB92B31.1FD4EF3E, state=4, offset=-2.328, frequency=18.704,
jitter=0.051, noise=0.735, stability=0.025'
```

SSL Medium Strength Cipher Suites Supported

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. GLESEC regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note: Reconfigure the affected application if possible to avoid use of medium strength ciphers

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Affected Systems

443 / tcp / cisco-ssl-vpn-svr 201.218.212.9, 201.218.212.35

443 / tcp / possible_wls 200.46.240.137,ec2-52-86-152-128.compute-

1.amazonaws.com

Output

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:

1. First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

2. Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

3. Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

4. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution
Purchase or generate a proper certificate for this service.

Affected Systems
443 / tcp / cisco-ssl-vpn-svr 201.218.212.9

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=201.218.212.9
|-Issuer  : CN=201.218.212.9
```

SSL Version 2 and 3 Protocol Detection

Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

1. An insecure padding scheme with CBC ciphers.

2. Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is

recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Affected Systems
443 / tcp / cisco-ssl-vpn-svr 201.218.212.9
Output

```
- SSLv3 is enabled and the server supports at least one cipher.
```

SSL Certificate Signed Using Weak Hashing Algorithm

Description
The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Solution
Contact the Certificate Authority to have the certificate reissued.

Affected Systems
443 / tcp / cisco-ssl-vpn-svr 201.218.212.9

Output

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : CN=201.218.212.9
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Aug 11 05:10:16 2017 GMT
|-Valid To            : Aug 09 05:10:16 2027 GMT
```

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE)

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Note: Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Solution

Disable SSLv3.

Affected Systems

443 / tcp / cisco-ssl-vpn-svr 201.218.212.9

Output

```
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key

Description

The remote Internet Key Exchange (IKE) version 1 service seems to support Aggressive Mode with Pre-Shared key (PSK) authentication. Such a configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks.

Solution

1. Disable Aggressive Mode if supported.
2. Do not use Pre-Shared key for authentication if it's possible.
3. If using Pre-Shared key cannot be avoided, use very strong keys.
4. If possible, do not allow VPN connections from any IP addresses.

Note that this plugin does not run over IPv6.

Affected Systems

500 / udp / ike 201.218.212.9

Low Risk Level Vulnerabilities

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Affected Systems

443 / tcp / possible_wls ec2-52-86-152-128.compute-1.amazonaws.com

Output

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    ECDHE-RSA-RC4-SHA            Kx=ECDH       Au=RSA      Enc=RC4(128)            Mac=SHA1
    RC4-MD5                      Kx=RSA        Au=RSA      Enc=RC4(128)            Mac=MD5
    RC4-SHA                      Kx=RSA        Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Affected Systems

443 / tcp / cisco-ssl-vpn-svr 201.218.212.9

Output

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-SHA                      Kx=RSA        Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Web Server Transmits Cleartext Credentials

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Affected Systems

8080 / tcp / possible_wls	ec2-52-72-43-239.compute-1.amazonaws.com
80 / tcp / possible_wls	ec2-52-72-43-239.compute-1.amazonaws.com

Output

```
Page : /examples/jsp/security/protected/index.jsp
Destination Page: /examples/jsp/security/protected/j_security_check

Page : /examples/jsp/security/protected
Destination Page: /examples/jsp/security/j_security_check
```

The low level vulnerabilities are related to the weak cipher suites such as RC4, RSA and also related to errors in SSL certificates.

GLESEC
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Whole Compiled Recommendations

GLESEC recommends for Copa Airlines to address the following

1. Take immediate actions to the detailed recommendations in this report.
2. Certificates that can be trusted or SSL Certificate Chain contains RSA keys less than 2048 bits should be corrected.
3. SSL medium Strength cipher suites should not be allowed for SSL connections.
4. Restrict NTP 6 mode queries to prevent unauthorized remote access.
5. Modify the affected CGI scripts (CGI Generic SQL Injection).
6. We recommend applying the most recent patches for your endpoints, since we have identified that 85% of the devices used for the TAS service have outdated software installed.
7. We recommend taking the necessary measures to solve the problem presented to the IP address 52.72.43.239 which presents a high vulnerability due to problems of CGI Generic SQL Injection (blind).

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com

www.glesec.com