OPERATIONS & INTELLIGENCE CYBER SECURITY REPORT

Copa Airlines

January, 2018

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

Info@glesec.com
www.glesec.com

CONFIDENCIAL

Table of Contents

CONFIDENTIAL

About This Report

The purpose of this document is to report on the "state" of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed. The more complete the set of services under contract the more accurate and complete the results will be.

The report is organized in three parts; the first is the Executive Summary with recommendations (as necessary or applicable), the second is the Intelligence Section with more detail information and analysis dashboards and the last is Operational Section with status of the services and counter-measures under contract, tickets for change management and incidents reported and consulting activity for the month.

We at GLESEC believe that information security is a holistic and dynamic process that requires on-going research and follow up and should be handled with the right tools, systems, processes, skill personnel and focus attention. The process is dynamic due to the constant discovery of new security vulnerabilities and exploits, the proliferation of hacking tools that make it easier for script-kiddies with minimal knowledge to cause damage. The increase in malware, phishing, insider threats, espionage, organized crime, intellectual property theft, and hacktivism are the very cause of information security exposure and are most commonly driven by financial gain. GLESEC's outsourcing services, based on its proprietary TIPTM platform portfolio provide the ideal response to the above.

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.

CONFIDENTIAL

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

Scope of this Report

GLESEC Contracted Services Table
This table list of GLESEC TIP™ services and indicate which are contracted and the corresponding service expiration dates of the contracts.

Type	Service	Contracted?	Service Expiration
Threat Mitigation	MSS-APS		
Threat Mitigation	MSS-APS-SSL		
Threat Mitigation	MSS-APS-PS		
Threat Mitigation	MSS-APFW		
Vulnerability Testing	MSS-VME	YES	11/30/2018
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM		
Risk assessment	MSS-BAS		
Threat Mitigation	MSS-EIR		
Threat Mitigation	MSS-UTM		
Threat Mitigation	MSS-INT		
Access Control	MSS-TAS	YES	11/30/2018

CONFIDENTIAL

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

Executive Summary

This report corresponds to the period from January 01 to January 31, 2018.

The following table describes the major categories that GLESEC has identified to report on the state-of-security of its member-clients. The categories in the table below are based on risk-management methodology. This is a principal foundational aspect of GLESEC.

RISK / RIESGO
VULNERABILITIES / VULNERABILIDADES • MSS-VM Service
THREATS / AMENAZAS • MSS-APS; MSS-EPS; MSS-SIEM; MSS-EIR; MSS-UTM
ASSETS / ACTIVOS • MSS-VM; MSS-EPS
COMPLIANCE / CUMPLIMIENTO • MSS-EPS
SECURITY VALIDATION / VALIDACION • MSS-BAS
TRUSTED ACCESS / ACCESS CON CONFIABILITIDAD • MSS-TAS

RISK

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. The NIST Cyber-Security Framework

One of GLESEC's foundational columns is basing all its activities to support RISK determination and mitigation. What any organization should want to know if what is their level of RISK, and in this case in particular to cyber-security. Cyber-Security RISK has a direct impact to the business and as such is of paramount importance to the Board and Management of the company.

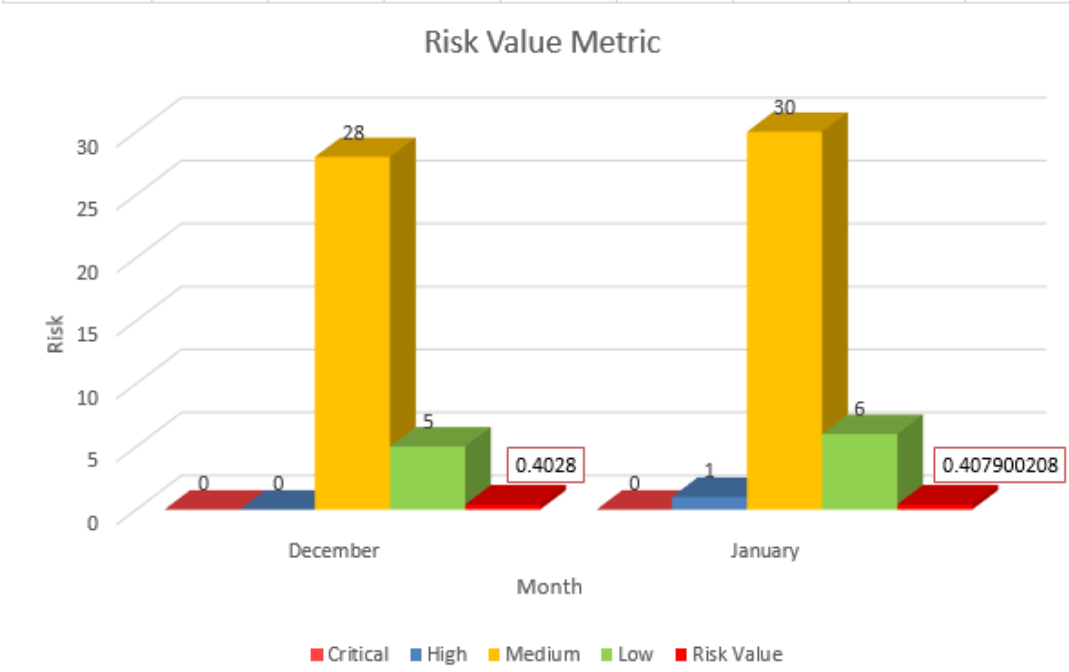
We at GLESEC measure RISK through a number of perspectives and using several of

CONFIDENTIAL

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

the TIP™ platform portfolio of services. The MSS-VM or Managed Vulnerability Service provides us with one view, how weak are the systems of the organization. The MSS-BAS provides us a view of how weak are the defenses of the organization to the latest threats. The MSS-APS, MSS-SIEM, MSS-UTM, MSS-EIR, MSS-EPS provides us with attack information both internal and external, DDOS, Malware, Ransomware and other attack vector information as well as provide protection level services. The MSS-EPS also provides us RISK level information for non-compliance with internal or external requirements and/or regulations. All in all a variety of services provide us with different views and together we have the most complete view of our client's security posture.

The RISK VALUE METRIC histogram below represents the changes in the Vulnerability based Risk Value Metric over the past six months.



VULNERABILITIES

GLESEC's MSS-VM(E/I) service is used to conduct two weekly testing to external and/or internal systems (depending on the options of the contracted service). Of the two tests performed weekly, one is to test for discovery of assets on the network and the other to test for vulnerabilities. The external testing is performed from GLESEC' cloud platform and the internal is conducted with the GLESEC Multi-security Appliance (GMSA).

CONFIDENTIAL

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

Vulnerabilities are weaknesses that if exploited can compromise the organization and as such are a component of RISK for the organization. If there are vulnerabilities and also threats there is RISK that the organization can be impacted. The vulnerabilities reported by GLESEC should be considered all important and addressed according to the priority (Critical, High, Medium and Low). An effective process is to work with the GLESEC provided information and GLESEC consulting team to address the recommendations provided in a systematic and continuous way. Progress can be determined by the weekly testing.

Overall the vulnerabilities for Copa Airlines this period have been very significant with 1 high and 35 medium vulnerabilities. The organization has a very high level of exposure and we urge Copa Airlines to take immediate action. Particular and urgent attention has to be concentrated on host 52.1.19.81, which represents a vulnerability related to GGI Generic SQL Injection.
The number of vulnerabilities remains approximately the same as prior month, just a few more, this suggests that more efforts have to be done to remediate these.

Risk Value Metric
GLESEC utilizes a metric to provide a way to quantify the vulnerabilities based risk of an organization. This metric is to measure the relative value of vulnerabilities and also the record of change over time.

It is important to mention that this metric considers a median value for the vulnerabilities classified as “critical”, “high”, “medium” and “low”, giving them a weight of 100%, 75%, 50% and 10% respectively.

This takes into consideration all of the vulnerabilities, but is important to point out that this values (100%, 75%, 50% and 10%) are arbitrarily chosen by us, so this measure can in time change as we understand more of the risks involved. We can use this metric to evaluate the progress in time and to compare one over the other using a common amount set.

The following external network ranges 201.218.212.35, 201.218.212.9, 201.218.212.162, 201.218.212.82, 201.218.212.30, 200.46.240.137, 200.46.241.161, 52.1.19.81, 52.3.92.27, 52.72.43.239, 52.86.152.128, 54.164.239.210, 34.199.239.56 for Copa Airlines were scanned for vulnerabilities.

The following table indicates the external vulnerability metric.

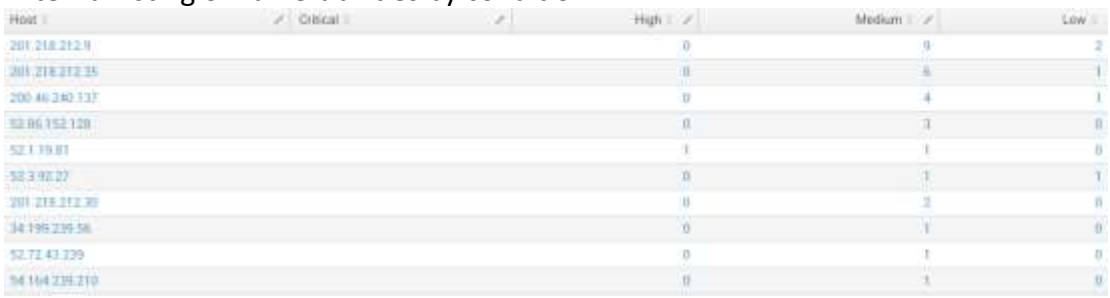
CONFIDENTIAL

Total IP's Scanned				IP's Vulnerable
13				12
Risk Distribution				
Critical	High	Medium	Low	Total
0	1	30	6	37

According to the metrics:
RV= 0.407900208

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

External listing of vulnerabilities by condition:



Host	Critical	High	Medium	Low
201.218.212.9		0	0	2
201.218.212.35		0	6	1
200.46.240.137		0	4	1
52.86.152.128		0	3	0
52.1.19.81		1	1	0
52.3.92.27		0	1	1
201.218.212.30		0	2	0
34.199.239.56		0	1	0
52.72.43.229		0	1	0
54.164.239.210		0	1	0

The following table provides a comparison of persistent external vulnerabilities of the current month and previous month.

host-ip	Previous Month	Current Month
200.46.240.137	5	5
200.46.241.161	1	1
201.218.212.30	2	2
201.218.212.35	7	7
201.218.212.62	1	1
201.218.212.9	11	11
34.199.239.56	1	1
52.1.19.81	1	2
52.3.92.27	2	2
52.72.43.229	1	1
52.86.152.128	3	3
54.164.239.210	1	1

Please view Recommendations for more details. This can be seen on the GLESEC MEMBER PORTAL (GMP).

CONFIDENTIAL

Vulnerability Categories

The following table indicates the categories that we use for vulnerabilities as a way to provide context to them and facilitate the prioritization of how to handle remediation.

Preliminary Analysis	Firewalls	Network Devices
SMB/NetBIOS	SSH Servers	Malformed Packets
Simple Network Services	Mail Servers	Proxy Servers
Policy Checks	SQL Servers	Wireless AP
Web Servers	FTP Servers	Webmail Servers
RPC Services	Server Side Scripts	NFS Services
Backdoors	SNMP Services	Printers
Encryption and Authentication	DNS Servers	

Based on the above the following table shows a matrix of the total External vulnerabilities by category.

Name	Critical	High	Medium	Low	Total
CGI abuses	14	12	2	0	28
FTP	0	4	0	0	4
General	0	0	31	8	39
Misc.	0	0	5	3	8
Service detection	0	0	7	0	7
Web Servers	6	4	11	0	21

TRUSTED ACCESS

The new IT model brings with it a greater attack surface, comprised by employees that use their own devices for work, while working remotely. The proliferation of cloud applications for nearly every business need has also contributed to increased technical complexity. These days, attackers can expose much different vulnerability in multiple vectors — in a single attack. Traditional security is designed to address separate, siloed attacks, making these solutions ineffective against modern threats. These new threats center on gaining remote access to your apps and data — whether it's with stolen passwords or exploited known vulnerabilities targeting your users, their out-of- date devices, cloud applications and remote access software.

The Managed Trusted Access Service (MSS-TAS) is a holistic security service to (a) ensure that the user's access is trusted (valid user) and (b) the devices used by the user to authenticate meet the organization's security standards.

CONFIDENTIAL

The Trusted Access as reported by the MSS-TAS for this month are 385 total users, of which 153 have been authenticated successfully, 193 have not enabled and 43 denied authentications. It is recommended to verify why the 43 denied authentications.

Recommendations

GLESEC recommends for Copa Airlines to address the following

1. Take immediate actions to the detailed recommendations in this report.
2. Consult the application's documentation to disable SSL 2.0 and 3.0.Use TLS 1.1 (with approved cipher suites) or higher instead.
3. Restrict NTP 6 mode queries to prevent unauthorized remote access.
4. Modify the affected CGI scripts (CGI Generic SQL Injection).
5. We recommend applying the necessary patches for your endpoints.

In our GLESEC Member-Client's Portal you will find more information about the affected hosts of the mentioned vulnerabilities.

Alert: All mentioned vulnerabilities have exploits available and are on the internet can be downloaded and used against you.

CONFIDENTIAL

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

Intelligence Section Per Service Module

Managed Vulnerability Service (MSS-VM) Intelligence Section

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.

The purpose of this section is to highlight intelligence gathered from this and other services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

The following graphs are dashboards generated by GLESEC's TIP™ platform. These dashboards are representative of metrics for this service.

It is important to establish a vulnerability management program as part of the information security strategy because soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their systems compromised.

Many of the vulnerabilities will provide CVE data. CVE (Common Vulnerabilities and Exposures) is a list of information security exposures and vulnerabilities sponsored by US-CERT and maintained by the MITRE Corporation. The CVE mission is to provide standard names for all publicly known security exposures as well as standard definitions for security terms. The CVE can be searched online at http://nvd.nist.gov/.

Vulnerability Score

The score of a vulnerability is determined by its risk factor; Critical, High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and

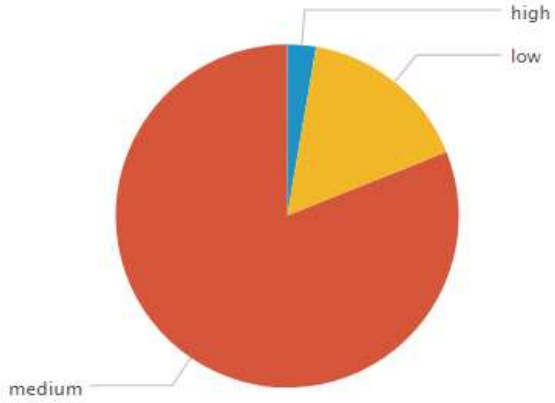
CONFIDENTIAL

coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of each vulnerability. In addition to numeric scores, the CVSS provides severity rankings of High, Medium, and Low but these qualitative rankings are simply mapped from the numeric CVSS scores. Vulnerabilities are labeled as:

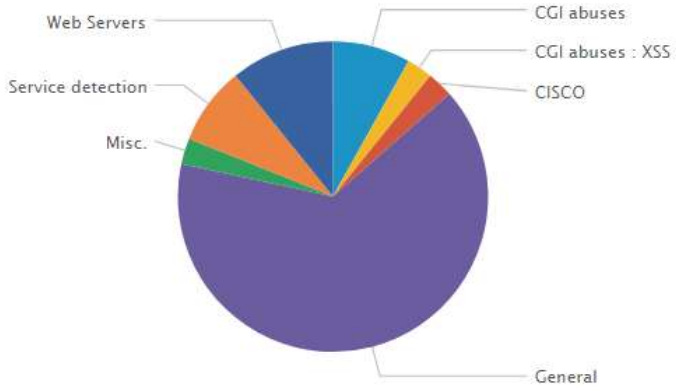
Low risk if they have a CVSS base score of 0.0 – 3.9
Medium risk if they have a CVSS base score of 4.0 – 6.9
High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period

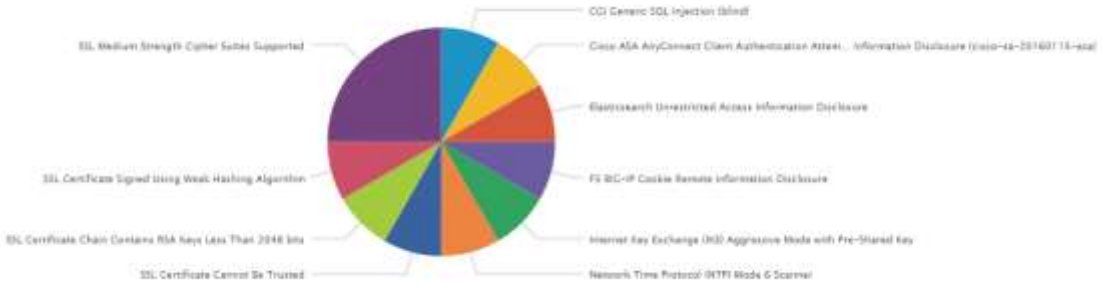


Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period

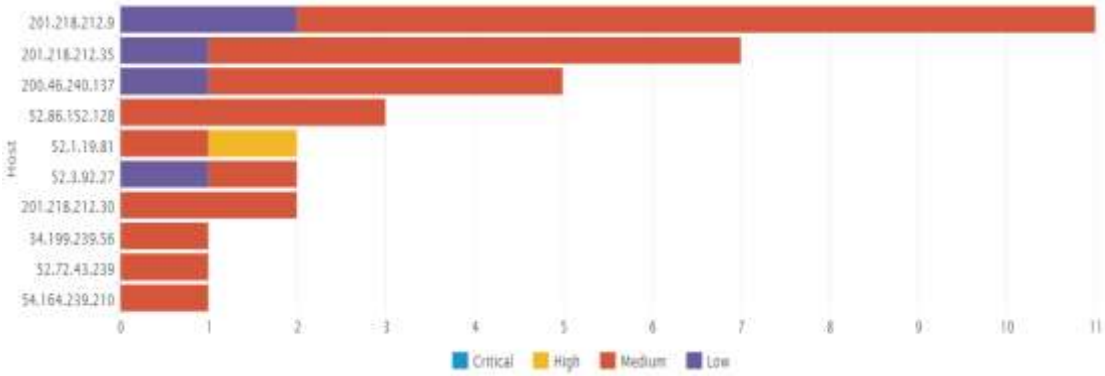


CONFIDENTIAL

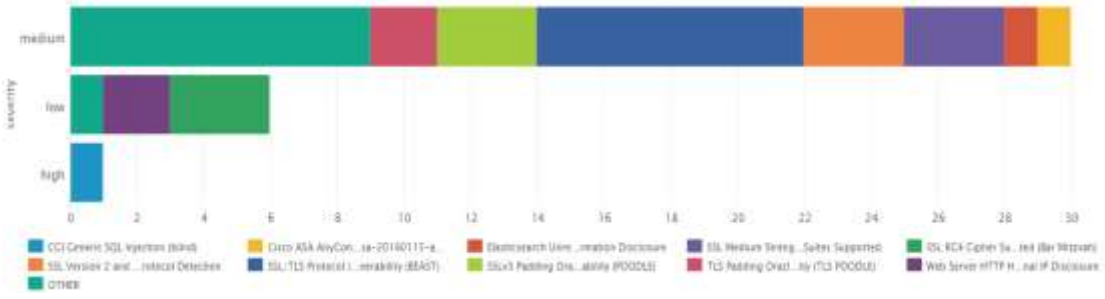
Graph: Most Frequent Vulnerability Name
This report depicts the most frequent vulnerabilities discovered this report period



Graph: Most Vulnerable Host
This report depicts the most vulnerable hosts discovered this report period



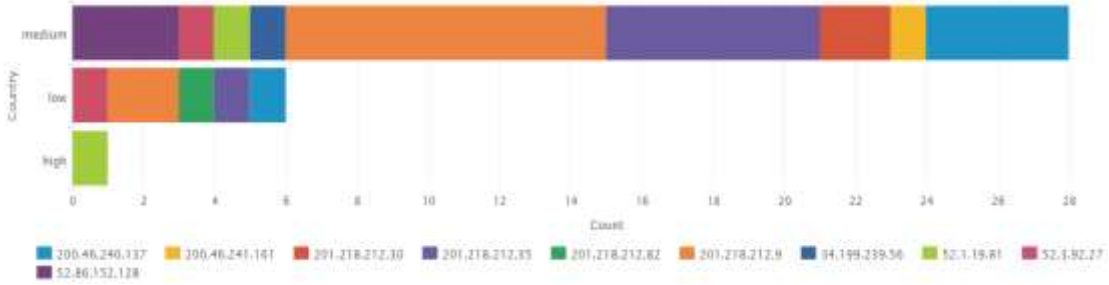
Graph: Vulnerability Risk by Vulnerability Name
This report illustrates the vulnerability risk and count by vulnerability name discovered this report period



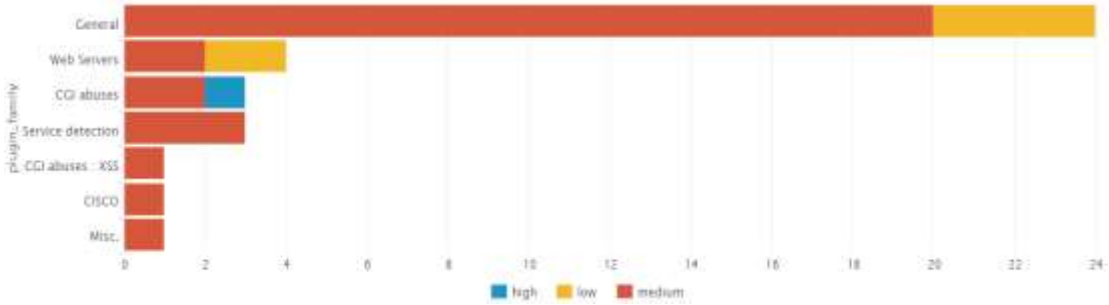
Graph: Vulnerability Risk by Host

CONFIDENTIAL

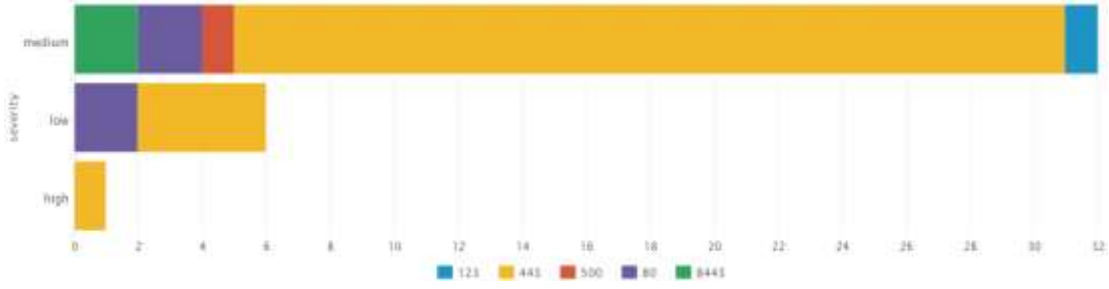
This report illustrates the vulnerability risk and count by category discovered this report period



Graph: Vulnerability Risk by Category
This report illustrates the vulnerability risk and count by category discovered this report period

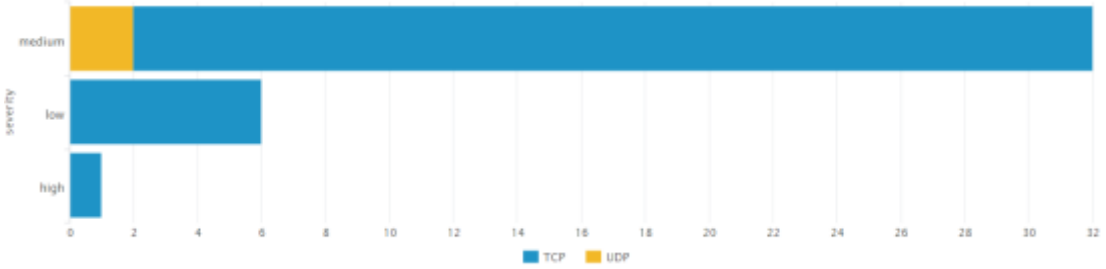


Graph: Vulnerability Risk by Port
This report illustrates the vulnerability risk and count by port discovered this report period

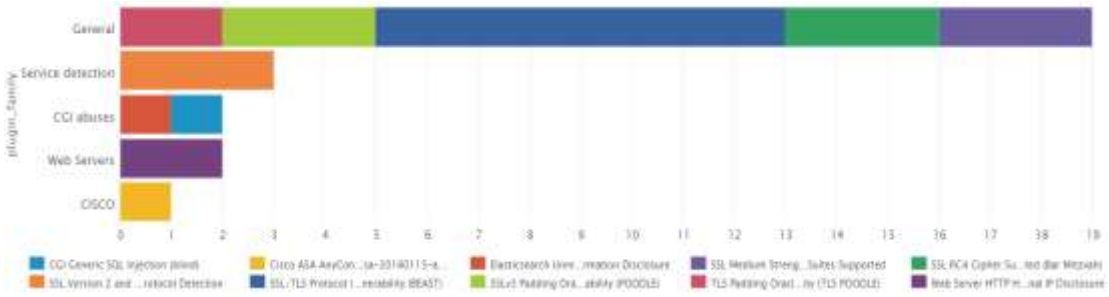


Graph: Vulnerability Risk by Protocol
This report illustrates the vulnerability risk and count by protocol discovered this report period

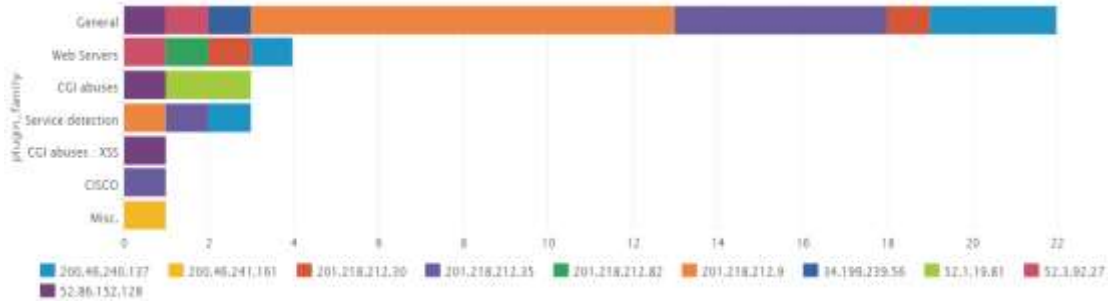
CONFIDENTIAL



Graph: Vulnerability Category by Vulnerability Name
This report illustrates the vulnerability category and count by vulnerability name discovered this report period

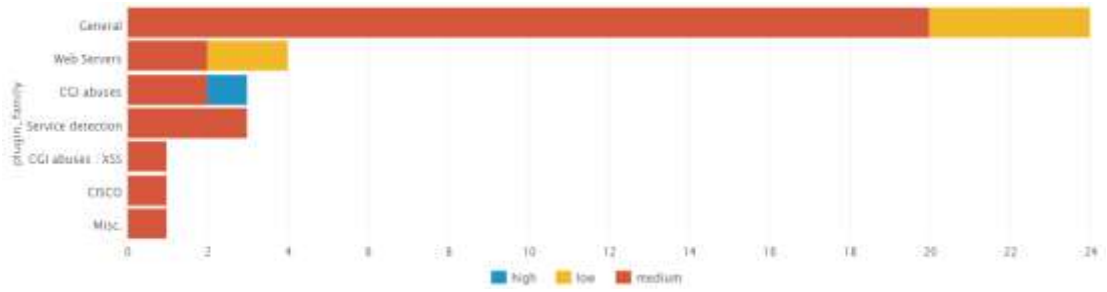


Graph: Vulnerability Category by Host
This report illustrates the vulnerability category and count by host discovered this report period

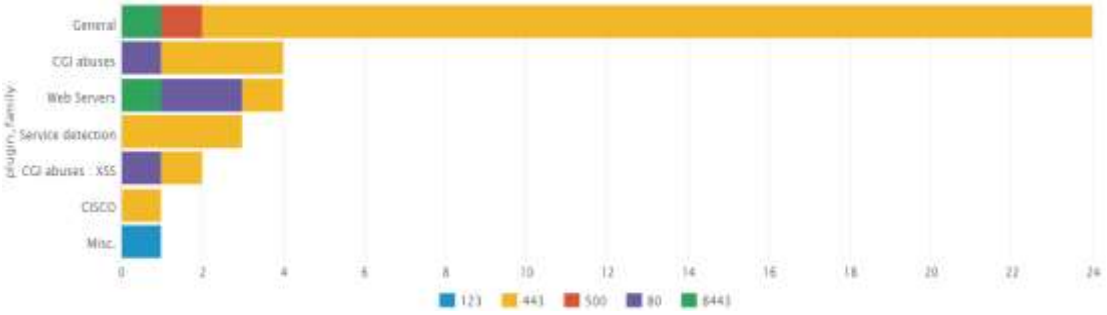


Graph: Vulnerability Category by Risk
This report illustrates the vulnerability category and count by risk discovered this report period

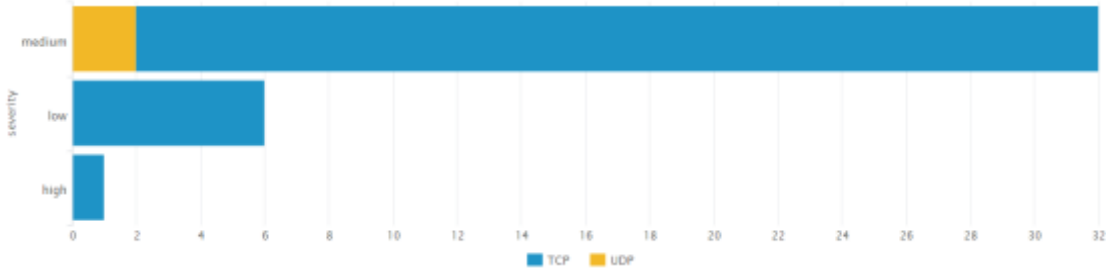
CONFIDENTIAL



Graph: Vulnerability Category by Port
This report illustrates the vulnerability category and count by port discovered this report period



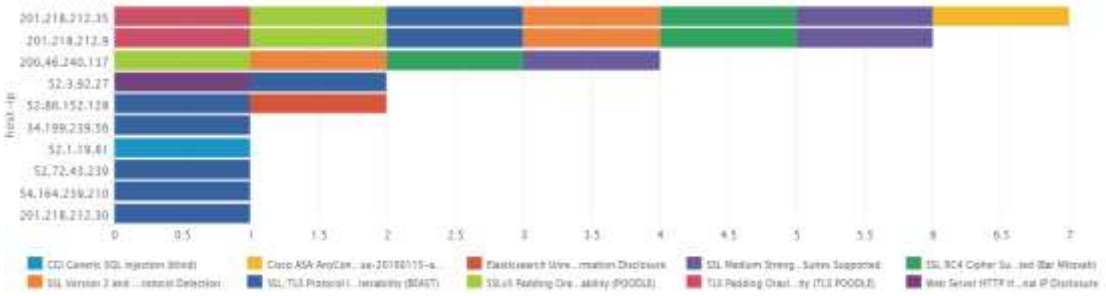
Graph: Vulnerability Category by Protocol
This report illustrates the vulnerability category and count by protocol discovered this report period



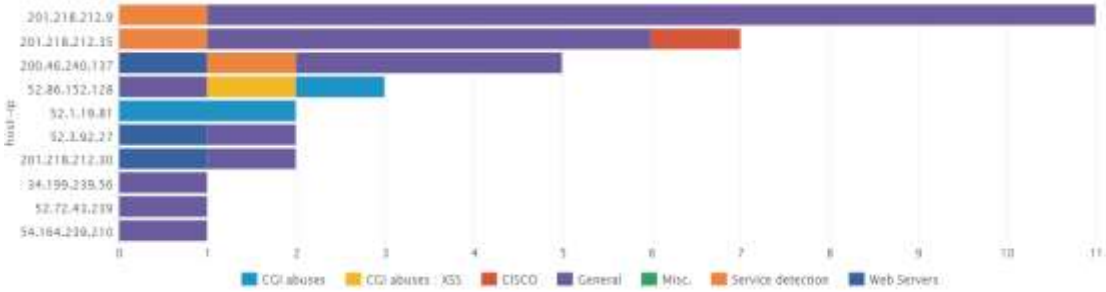
Graph: Host by Vulnerability Name
This report illustrates the vulnerability name and count by hosts discovered this report period

CONFIDENTIAL

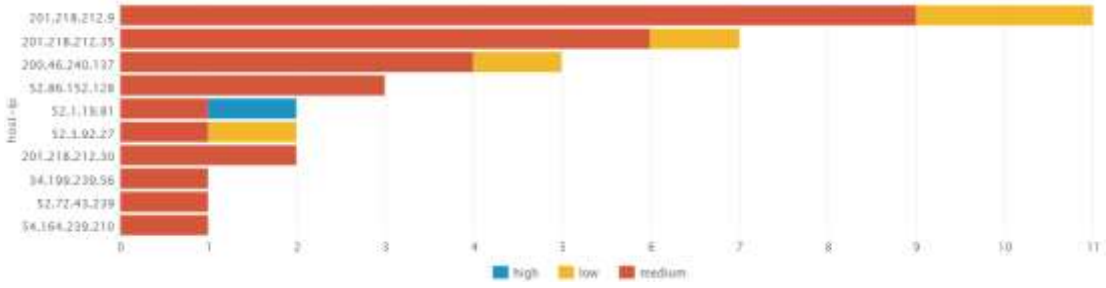
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



Graph: Host by Vulnerability Category
This report illustrates the vulnerability category and count by hosts discovered this report period

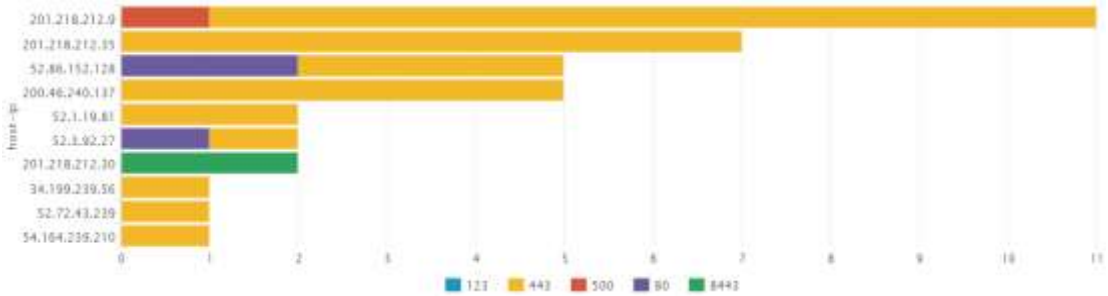


Graph: Host by Vulnerability Risk
This report illustrates the vulnerability risk and count by hosts discovered this report period

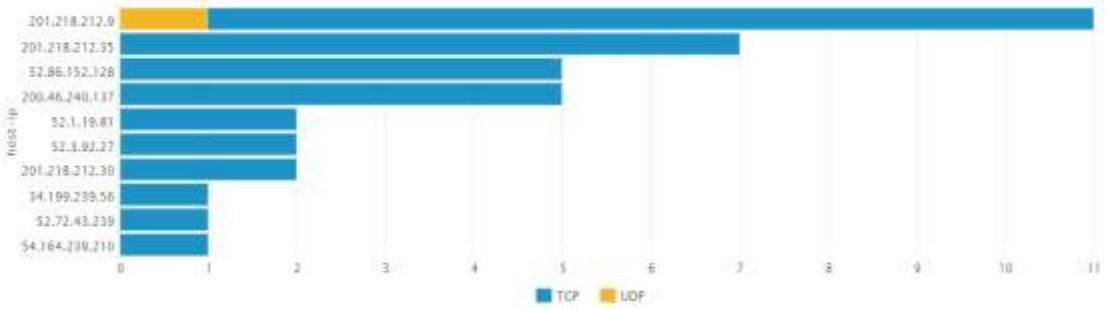


Graph: Host by Port
This report illustrates the port and count by hosts discovered this report period

CONFIDENTIAL



Graph: Host by Protocol
This report illustrates the protocol and count by hosts discovered this report period



CONFIDENTIAL

Managed Trusted Access Service (MSS-TAS) Intelligence Section

The Managed Trusted Access Service (MSS-TAS) is a holistic security service to (a) ensure that the users access is trusted (valid user) and (b) the devices used by the user to authenticate meet the organization's security standards. This is achieved by GLESEC's cloud-based service, part of the TIP™ platform.

The purpose of this section is to highlight intelligence gathered from this and other services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

The following graphs are dashboards generated by GLESEC's TIP™ platform. These dashboards are representative of metrics for this service.

Graph: User two-factor authentication.
This graph shows the total users using two factor authentication on your network.

385

Graph: Total Endpoints.
This graph shows the number of different endpoints used to access your organization system during this period.

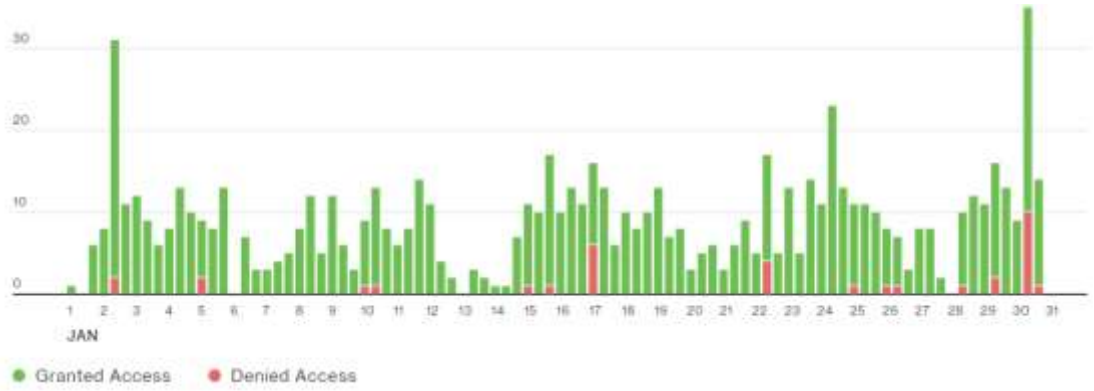
127

Graph: Endpoints out of date
This graph shows the number of devices that do not have the most recent updates installed.

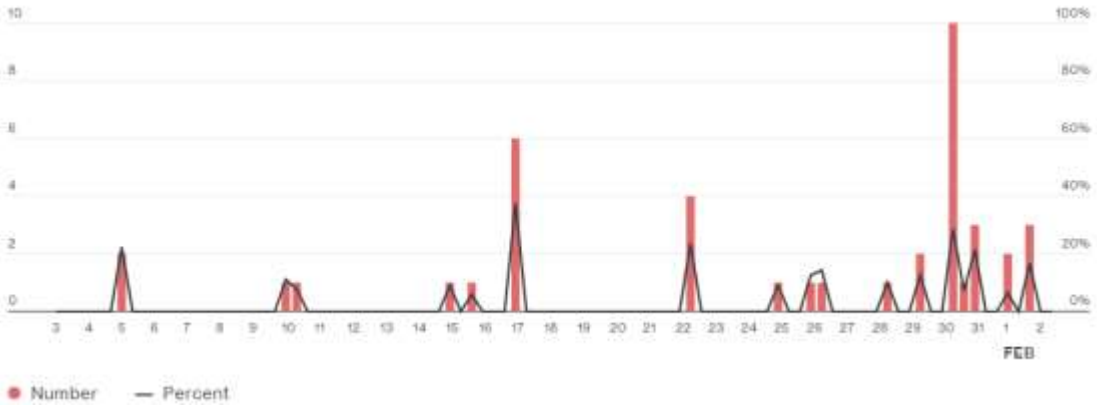
109

Graph: This Graph shows the IDs allowed and denied per month

CONFIDENTIAL

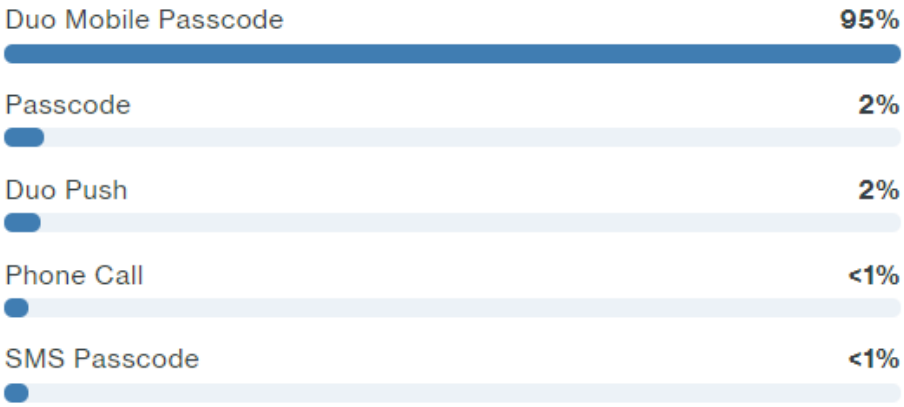


Graph: Denied Authentications



Graph: Successful Authentications by Factor over the Last Week

This graph shows the proportion of successful access granted by Push, Bypass code and mobile passcode



CONFIDENTIAL

TICKET ACTIVITY

In this section we report on all the change management and incidents tickets for the month.

Incidents Reported to the client During January 2018[..]

Ticket#	Title	Priority
2018020610000041	Notificación de Incidente (Copa)	2 high

CONFIDENTIAL

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

Definitions

A more complete list is available on the GMP portal

High Vulnerabilities are defined as being in one or more of the following categories: Backdoors, full Read/Write access to files, remote Command Execution, Potential Trojan Horses, or critical Information Disclosure (e.g. passwords).

Medium Vulnerabilities describes vulnerabilities that either expose sensitive data, directory browsing and traversal, disclosure of security controls, facilitate unauthorized use of services or denial of service to an attacker.

Low Vulnerabilities describes vulnerabilities that allow preliminary or sensitive information gathering for an attacker or pose risks that are not entirely security related but maybe used in social engineering or similar attacks.

SMB/NetBIOS vulnerabilities could allow remote code execution on affected systems. An attacker who successfully exploits these vulnerabilities could install programs; view, change, or delete data; or create new accounts with full user rights. Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

Simple Network vulnerabilities affect protocols like NTP, ICMP and common network applications like SharePoint among others. This is not meant to be a comprehensive list.

Authentication and encryption are two intertwined technologies that help to insure that your data remains secure. Authentication is the process of insuring that both ends of the connection are in fact “who” they say they are. This applies not only to the entity trying to access a service (such as an end user) but to the entity providing the service, as well (such as a file server or Web site). Encryption helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well.

While authentication and encryption each has its own responsibilities in securing a communication session, maximum protection can only be achieved when the two are combined. For this reason, many security protocols contain both authentication and encryption specifications.

CONFIDENTIAL

Authentication and encryption are two intertwined technologies that help to insure that your data remains secure. Authentication is the process of insuring that both ends of the connection are in fact “who” they say they are. This applies not only to the entity trying to access a service (such as an end user) but to the entity providing the service, as well (such as a file server or Web site). Encryption helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well.

While authentication and encryption each has its own responsibilities in securing a communication session, maximum protection can only be achieved when the two are combined. For this reason, many security protocols contain both authentication and encryption specifications.

CONFIDENTIAL

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

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

Info@glesec.com
www.glesec.com