



Your Global Cyber-Security Partner

**ON-DEMAND
OPERATIONS & INTELLIGENCE (MO&I) TECHNICAL REPORT
TLP-AMBER**

OCFL

November 23, 2022



USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
TEL: +1 (609) 651-4246 | +1(321)430-0500 | +(507) 836-5355

About This Report

This on-demand technical report is compiled for the people with responsibility for Cyber Security, Networking, Databases, Compliance, Infrastructure and Systems. A more detail monthly report is prepared and available from the Orchestration platform (GMP). For any questions about this report please contact the GLESEC Operation Centers (GOCs).

Managed Vulnerability Service (MSS-VM) Section

The Managed Vulnerability Service (MSS-VM) is a “Security as a service” (SaaS) offering to identify network assets, test, validate, correlate and report on vulnerabilities in a lifecycle process that integrates with GLESEC’s Orchestration platform. This integration provides for the optimization of the time and costs it takes an organization to remediate its business relevant vulnerabilities.

The Risk Value (see definition below) for OCFL for this period can be seen in the following chart.

VULNERABILITY LEVEL COLOR



The following table indicates the vulnerability metrics including total discovered systems, total vulnerable systems, and Risk Value (RV). The RV is defined as a weighted average of vulnerabilities.

The following values are to clarify the RV:

RV=1 Points to every IP address in the infrastructure that is susceptible to attacks

RV=0 Points to no IP address in the infrastructure that is susceptible to attacks

RV=0.1 Points to 1/10 IP address in the infrastructure that is susceptible to attacks

TOTAL DISCOVERED HOSTS

71

TOTAL VULNERABLE HOSTS

14

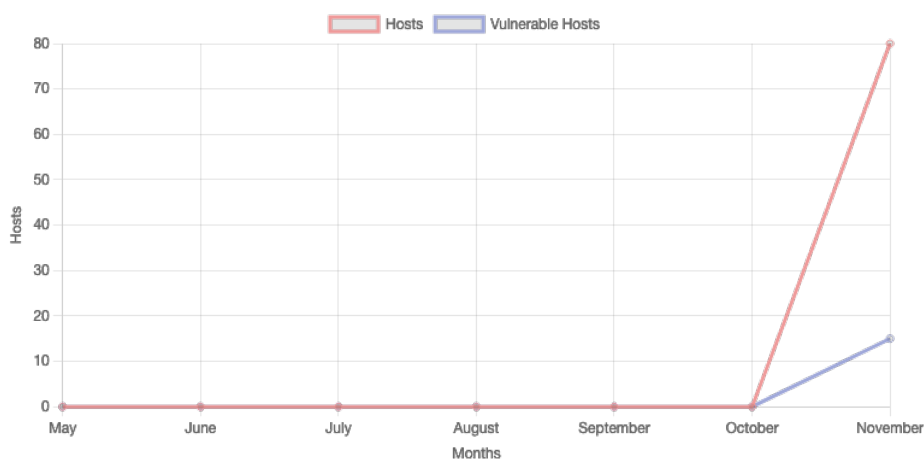
EXECUTIVE SUMMARY RISK DISTRIBUTION

Scanner	critical	high	medium	low	Total
OCFL	4		42	4	50

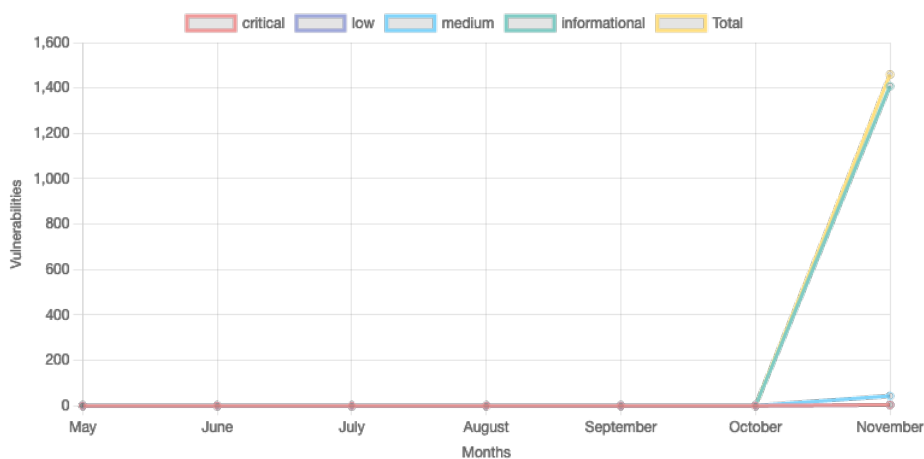
All the vulnerabilities found in your organization belong to the following categories:

The following graphs show the histograms for the last 6 months: Vulnerability Histogram, Vulnerability/Severity, Discovered Network Assets and the last one shows the Comparison of the number of Vulnerabilities between the Previous Month and the Current Month

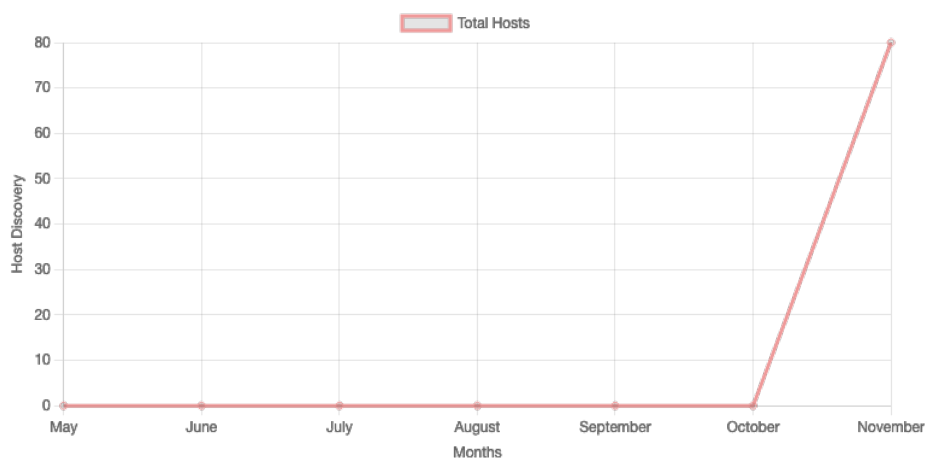
VULNERABILITY HISTOGRAM - FOR 6 MONTHS



VULNERABILITY SEVERITY HISTOGRAM - FOR 6 MONTHS



DISCOVERED NETWORK ASSET HISTOGRAM - FOR 6 MONTHS



COMPARISON VULNERABILITIES

n/a

The following graphs show the distribution of the vulnerabilities found on your servers or endpoints

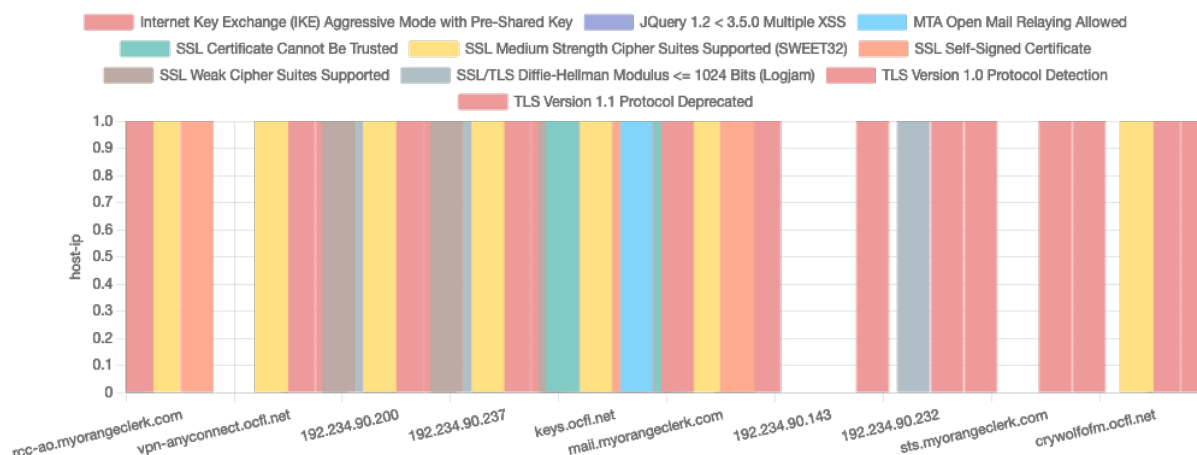
VULNERABILITY CATEGORY BY RISK

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

category	critical	low	medium
General	0	0	22
Service detection	2	0	17
Misc.	0	4	0
CGI abuses : XSS	0	0	2
SMTP problems	2	0	0
Backdoors	0	0	1

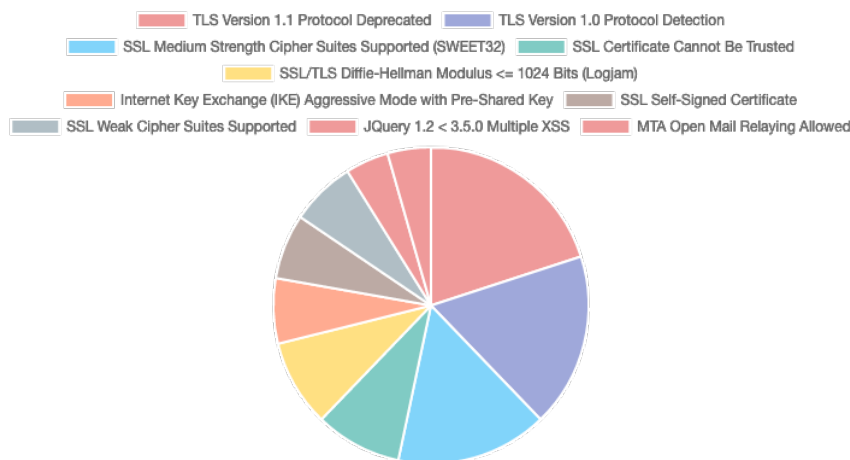
HOST BY VULNERABILITY NAME

This report illustrates the vulnerability name and count by hosts discovered this report period



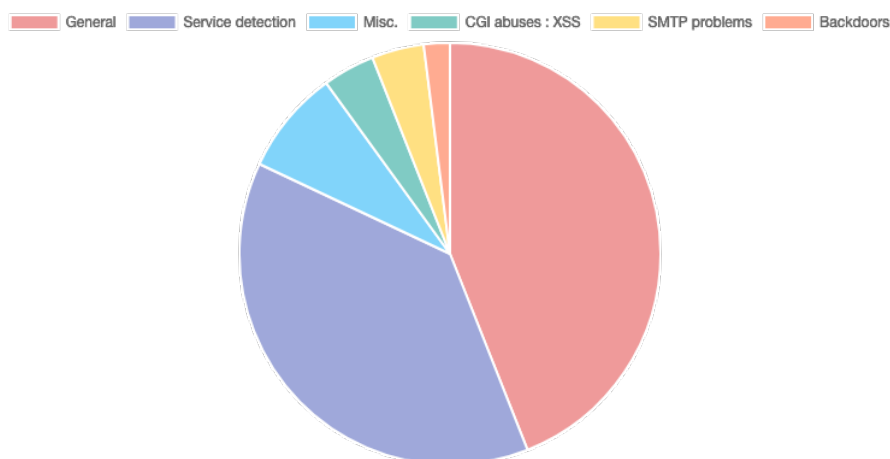
MOST FREQUENT VULNERABILITY NAME

This report depicts the most frequent vulnerabilities discovered this report period



MOST FREQUENT VULNERABILITY CATEGORY

This report depicts the most frequent vulnerabilities by category discovered this report period



The following graphs show the distribution of the vulnerabilities found on your servers or endpoints

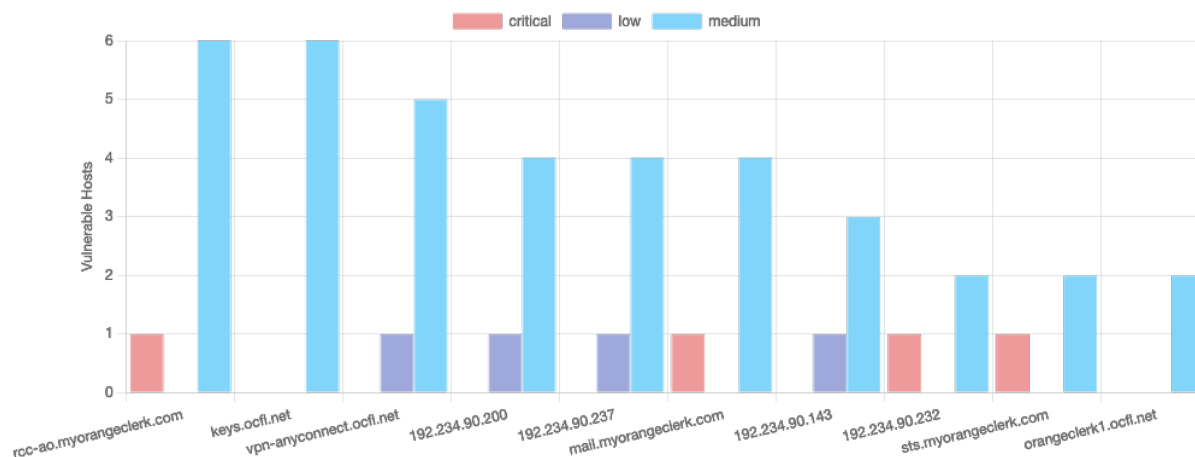
HOST BY PROTOCOL

This report illustrates the protocol and count by hosts discovered this report period

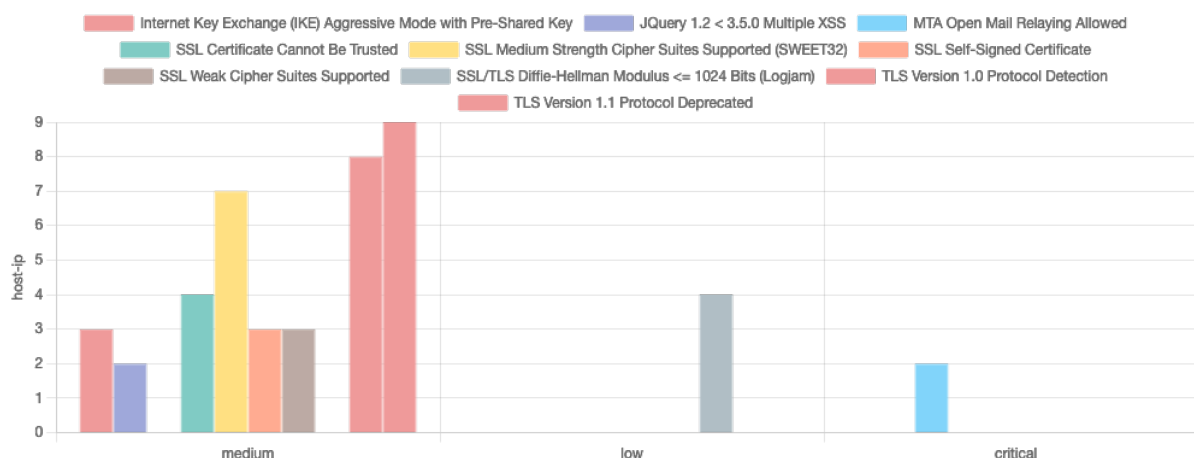
n/a

HOSTS BY RISK

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



VULNERABILITY RISK BY VULNERABILITY



VULNERABILITY CATEGORY BY PROTOCOL

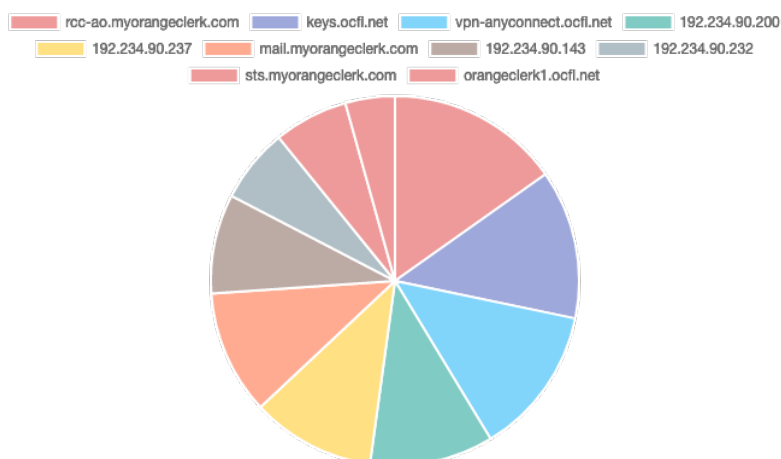
This report illustrates the vulnerability category and count by protocol discovered this report period

n/a

The following graphs show the distribution of the vulnerabilities found on your servers or endpoints

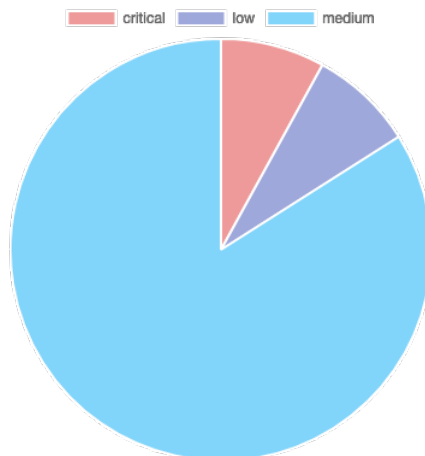
MOST VULNERABLE HOST

This report depicts the most vulnerable hosts discovered this report period



RISK DISTRIBUTION

This shows the risk distribution of vulnerabilities discovered for this period



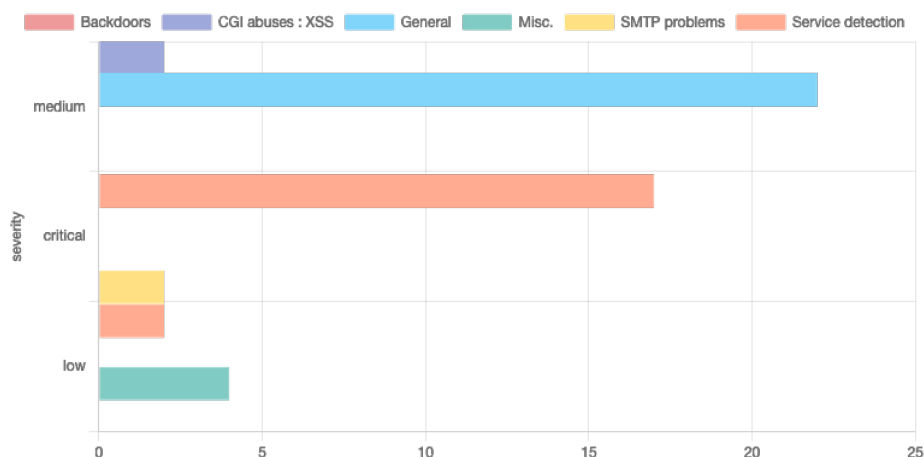
HOST BY VULNERABILITY CATEGORY

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



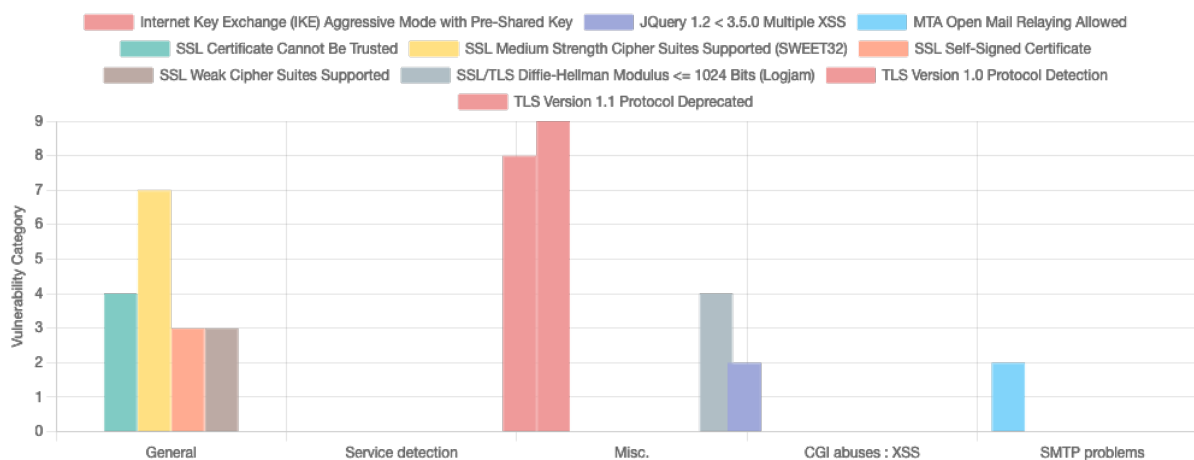
VULNERABILITY RISK BY VULNERABILITY CATEGORY

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



VULNERABILITY CATEGORY BY VULNERABILITY NAME

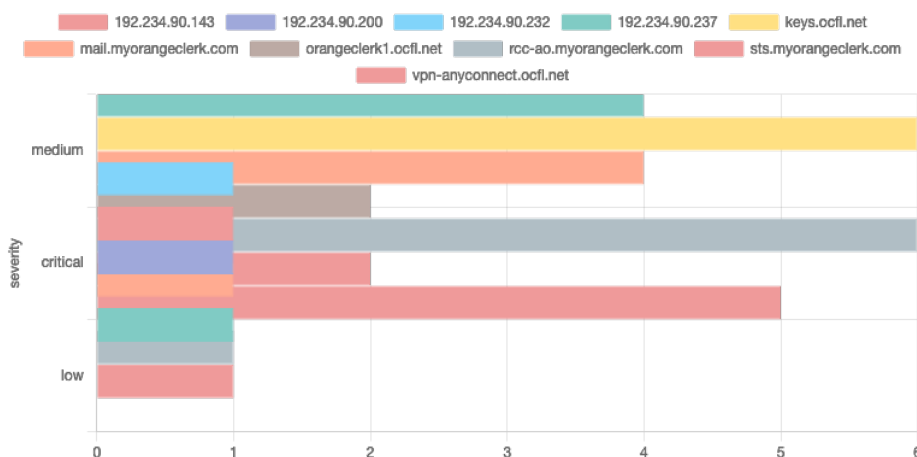
This report illustrates the vulnerability category and count by vulnerability name discovered this report period



The following graphs show the distribution of the vulnerabilities found on your servers or endpoints

VULNERABILITY RISK BY HOST

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



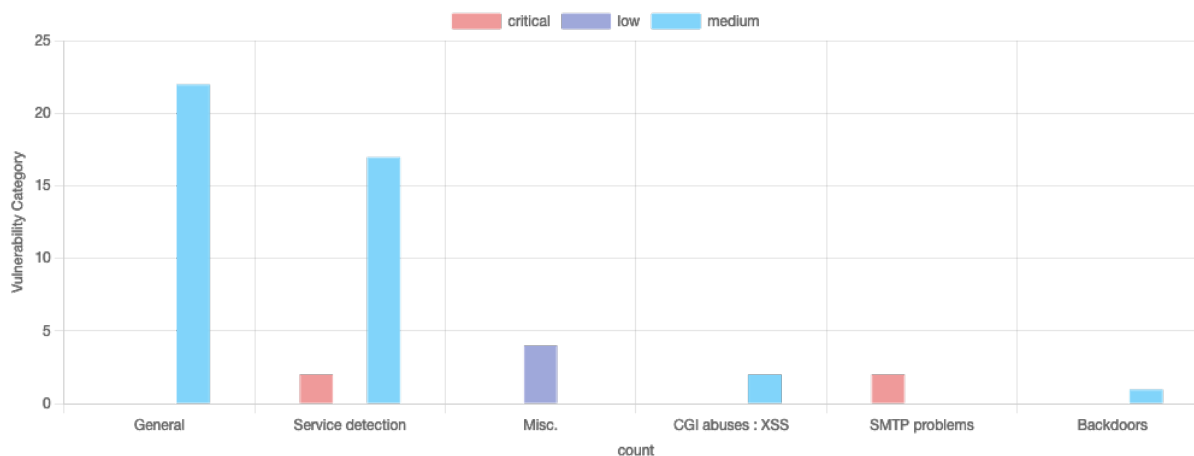
VULNERABILITY RISK BY PORT

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

n/a

VULNERABILITY CATEGORY BY RISK

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



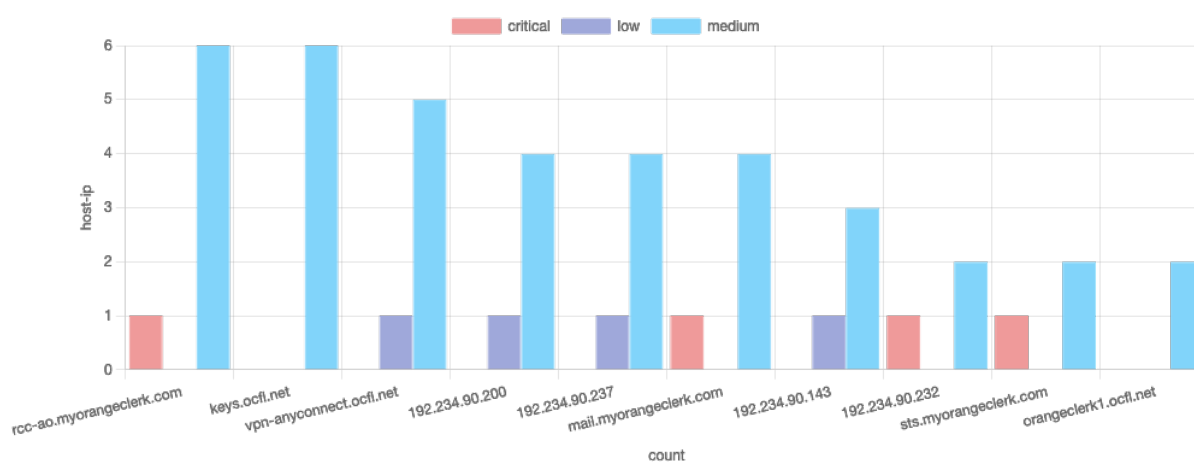
VULNERABILITY CATEGORY BY PORT

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

n/a

HOST BY VULNERABILITY RISK

The following illustrates the vulnerability risk and count by hosts discovered this report period



HOST BY PORT

The following graph illustrates the port and count by hosts discovered this report period

n/a

VULNERABILITIES & ASSETS CORRELATION

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Medium	192.234.90.93	Microsoft Windows Server 2012	vm.ocfl.net	Not Set	Not Set	JQuery 1.2 < 3.5.0 Multiple XSS	136929	true	2020/04/29	02 day(s)	2022/11/22 04:23:12-0500
Medium	Medium	192.234.90.233		mail.myorangeclerk.com	Not Set	Not Set	SSL Certificate Cannot Be Trusted	51192	n/a	n/a	02 day(s)	2022/11/22 04:13:43-0500
Medium	Medium	192.234.90.233		mail.myorangeclerk.com	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	02 day(s)	2022/11/22 04:13:43-0500
Medium	Critical	192.234.90.232	Microsoft Windows Server 2012 R2	Unknown	Not Set	Not Set	SSL Version 2 and 3 Protocol Detection	20007	n/a	n/a	02 day(s)	2022/11/22 04:09:41-0500
Medium	Medium	192.234.90.232	Microsoft Windows Server 2012 R2	Unknown	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	02 day(s)	2022/11/22 04:09:41-0500
Medium	Medium	192.234.90.232	Microsoft Windows Server 2012 R2	Unknown	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:09:41-0500
Medium	Medium	192.234.90.237	CISCO ASA 5500	Unknown	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	02 day(s)	2022/11/22 04:09:32-0500
Medium	Medium	192.234.90.142	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	62694	false	2002/09/03	02 day(s)	2022/11/22 04:09:26-0500
Medium	Medium	192.234.90.142	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	02 day(s)	2022/11/22 04:09:26-0500
Medium	Medium	192.234.90.142	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:09:26-0500
Low	Low	192.234.90.142	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	83875	n/a	n/a	02 day(s)	2022/11/22 04:09:26-0500
Medium	Medium	192.234.90.235	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	02 day(s)	2022/11/22 04:09:11-0500

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Medium	192.234.90.65	Juniper SSL VPN Appliance	keys.ocfl.net	Not Set	Not Set	SSL Certificate Cannot Be Trusted	51192	n/a	n/a	02 day(s)	2022/11/22 04:27:17-0500
Medium	Medium	192.234.90.65	Juniper SSL VPN Appliance	keys.ocfl.net	Not Set	Not Set	SSL Certificate Expiry	15901	n/a	n/a	02 day(s)	2022/11/22 04:27:17-0500
Medium	Medium	192.234.90.65	Juniper SSL VPN Appliance	keys.ocfl.net	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	02 day(s)	2022/11/22 04:27:17-0500
Medium	Medium	192.234.90.7	Microsoft Windows 10	crywolfofm.ocfl.net	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	02 day(s)	2022/11/22 04:23:20-0500
Medium	Medium	192.234.90.78	Microsoft Windows Server 2012 R2	ocarcims.ocfl.net	Not Set	Not Set	JQuery 1.2 < 3.5.0 Multiple XSS	136929	true	2020/04/29	02 day(s)	2022/11/22 04:21:46-0500
Medium	Critical	192.234.90.233		mail.myorangeclerk.com	Not Set	Not Set	MTA Open Mail Relaying Allowed	10262	false	1990/01/01	02 day(s)	2022/11/22 04:13:43-0500
Medium	Medium	192.234.90.233		mail.myorangeclerk.com	Not Set	Not Set	SSL Self- Signed Certificate	57582	n/a	n/a	02 day(s)	2022/11/22 04:13:43-0500
Medium	Medium	192.234.90.233		mail.myorangeclerk.com	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:13:43-0500
Medium	Medium	192.234.90.237	CISCO ASA 5500	Unknown	Not Set	Not Set	SSL Weak Cipher Suites Supported	26928	n/a	n/a	02 day(s)	2022/11/22 04:09:32-0500
Medium	Medium	192.234.90.237	CISCO ASA 5500	Unknown	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	02 day(s)	2022/11/22 04:09:32-0500
Medium	Medium	192.234.90.237	CISCO ASA 5500	Unknown	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:09:32-0500
Low	Low	192.234.90.237	CISCO ASA 5500	Unknown	Not Set	Not Set	SSL/TLS Diffie- Hellman Modulus <= 1024 Bits (Logjam)	83875	n/a	n/a	02 day(s)	2022/11/22 04:09:32-0500
Medium	Medium	192.234.90.235	CISCO ASA 5500	vpn- anyconnect.ocfl.net	Not Set	Not Set	SSL Weak Cipher Suites Supported	26928	n/a	n/a	02 day(s)	2022/11/22 04:09:11-0500
Medium	Medium	192.234.90.235	CISCO ASA 5500	vpn- anyconnect.ocfl.net	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	02 day(s)	2022/11/22 04:09:11-0500
Medium	Medium	192.234.90.235	CISCO ASA 5500	vpn- anyconnect.ocfl.net	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:09:11-0500

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Critical	192.234.90.187	Microsoft Windows Server 2012 R2	rcc-ao.myorangeclerk.com	Not Set	Not Set	MTA Open Mail Relaying Allowed	10262	false	1990/01/01	01 day(s)	2022/11/22 04:37:32-0500
Medium	Medium	192.234.90.187	Microsoft Windows Server 2012 R2	rcc-ao.myorangeclerk.com	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	01 day(s)	2022/11/22 04:37:32-0500
Medium	Medium	192.234.90.187	Microsoft Windows Server 2012 R2	rcc-ao.myorangeclerk.com	Not Set	Not Set	SSL Self-Signed Certificate	57582	n/a	n/a	01 day(s)	2022/11/22 04:37:32-0500
Medium	Medium	192.234.90.187	Microsoft Windows Server 2012 R2	rcc-ao.myorangeclerk.com	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	01 day(s)	2022/11/22 04:37:32-0500
Medium	Medium	192.234.90.187	Microsoft Windows Server 2012 R2	rcc-ao.myorangeclerk.com	Not Set	Not Set	SMTP Server Non-standard Port Detection	18391	n/a	n/a	01 day(s)	2022/11/22 04:37:32-0500
Medium	Medium	192.234.90.187	Microsoft Windows Server 2012 R2	rcc-ao.myorangeclerk.com	Not Set	Not Set	SSL Certificate Cannot Be Trusted	51192	n/a	n/a	01 day(s)	2022/11/22 04:37:32-0500
Medium	Medium	192.234.90.187	Microsoft Windows Server 2012 R2	rcc-ao.myorangeclerk.com	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	01 day(s)	2022/11/22 04:37:32-0500
Medium	Medium	192.234.90.246		ocvpn.ocfl.net	Not Set	Not Set	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	62694	false	2002/09/03	01 day(s)	2022/11/22 04:36:15-0500
Medium	Medium	192.234.90.200	CISCO ASA 5500	Unknown	Not Set	Not Set	SSL Weak Cipher Suites Supported	26928	n/a	n/a	01 day(s)	2022/11/22 04:34:53-0500
Medium	Medium	192.234.90.200	CISCO ASA 5500	Unknown	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	01 day(s)	2022/11/22 04:34:53-0500
Medium	Medium	192.234.90.200	CISCO ASA 5500	Unknown	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	01 day(s)	2022/11/22 04:34:53-0500
Low	Low	192.234.90.200	CISCO ASA 5500	Unknown	Not Set	Not Set	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	83875	n/a	n/a	01 day(s)	2022/11/22 04:34:53-0500
Medium	Critical	192.234.90.174	Microsoft Windows Server 2012 R2	sts.myorangeclerk.com	Not Set	Not Set	SSL Version 2 and 3 Protocol Detection	20007	n/a	n/a	02 day(s)	2022/11/22 04:31:36-0500
Medium	Medium	192.234.90.174	Microsoft Windows Server 2012 R2	sts.myorangeclerk.com	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	02 day(s)	2022/11/22 04:31:36-0500
Medium	Medium	192.234.90.174	Microsoft Windows Server 2012 R2	sts.myorangeclerk.com	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:31:36-0500

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Low	Low	192.234.90.235	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	83875	n/a	n/a	02 day(s)	2022/11/22 04:09:11-0500
Medium	Medium	192.234.90.141	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	62694	false	2002/09/03	02 day(s)	2022/11/22 04:09:10-0500
Medium	Medium	192.234.90.141	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	02 day(s)	2022/11/22 04:09:10-0500
Medium	Medium	192.234.90.141	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:09:10-0500
Low	Low	192.234.90.141	CISCO ASA 5500	vpn-anyconnect.ocfl.net	Not Set	Not Set	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	83875	n/a	n/a	02 day(s)	2022/11/22 04:09:10-0500
Medium	Medium	192.234.90.143	CISCO ASA 5500	Unknown	Not Set	Not Set	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	62694	false	2002/09/03	02 day(s)	2022/11/22 04:09:06-0500
Medium	Medium	192.234.90.143	CISCO ASA 5500	Unknown	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	02 day(s)	2022/11/22 04:09:06-0500
Medium	Medium	192.234.90.143	CISCO ASA 5500	Unknown	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:09:06-0500
Low	Low	192.234.90.143	CISCO ASA 5500	Unknown	Not Set	Not Set	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	83875	n/a	n/a	02 day(s)	2022/11/22 04:09:06-0500
Medium	Medium	192.234.90.200	CISCO ASA 5500	Unknown	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	01 day(s)	2022/11/22 04:34:53-0500
Medium	Medium	192.234.90.101	Juniper SSL VPN Appliance	orangeclerk1.ocfl.net	Not Set	Not Set	SSL Certificate Cannot Be Trusted	51192	n/a	n/a	02 day(s)	2022/11/22 04:32:44-0500
Medium	Medium	192.234.90.101	Juniper SSL VPN Appliance	orangeclerk1.ocfl.net	Not Set	Not Set	SSL Certificate Expiry	15901	n/a	n/a	02 day(s)	2022/11/22 04:32:44-0500
Medium	Medium	192.234.90.65	Juniper SSL VPN Appliance	keys.ocfl.net	Not Set	Not Set	TLS Version 1.0 Protocol Detection	104743	n/a	n/a	02 day(s)	2022/11/22 04:27:17-0500
Medium	Medium	192.234.90.65	Juniper SSL VPN Appliance	keys.ocfl.net	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	02 day(s)	2022/11/22 04:27:17-0500
Medium	Medium	192.234.90.65	Juniper SSL VPN Appliance	keys.ocfl.net	Not Set	Not Set	SSL Self-Signed Certificate	57582	n/a	n/a	02 day(s)	2022/11/22 04:27:17-0500

The table above represents the Vulnerabilities for the top 20 by Priority.

Cases Activity

Below is a histogram of the average time to resolve for the past six months and a list of cases with their time of resolution (including the time until now of cases that are not yet closed). For more details log-on the GMP and review the C&RU area.

MONTHLY RESPOND & RESOLVE AVG. TIMES

loading...

GLESEC Information Sharing Protocol

GLESEC REPORTS are in compliance with the U.S. Department of Homeland Security (DHS) Traffic-Light Protocol (TLP): TLP-White (Disclosure is Not Limited), TLP-Green (Limited Disclosure, Restricted Only to the Community), TLP-Amber (Limited Disclosure, restricted to the Participant's Organization), and TLP-Red (Not for Disclosure, Restricted/Classified - Only Shared with US DHS).



Your Global Cyber-Security Partner

GLESEC

**USA - ARGENTINA - PANAMA
MEXICO - BRAZIL - PERU - CHILE**

Tel: +1(609)651-4246

Tel: +1(321)430-0500

Tel: +(507)836-5355

info@glesec.com

www.glesec.com

