Your Global Cyber-Security Partner

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

TLP-AMBER

GLESEC

September 27, 2021

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 GLESEC for this period can be seen in the following chart.

RISK 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

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

TOTAL VULNERABLE HOSTS

18

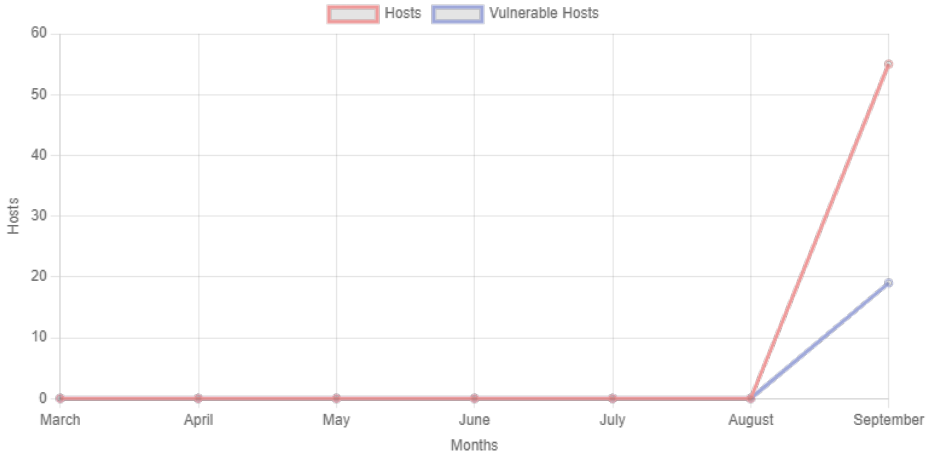
EXECUTIVE SUMMARY RISK DISTRIBUTION

	Scan Name	High	Low	Medium	Total
1	GLESEC	7	1	41	49
2	GLESEC WEB SERVERS	0	0	1	1

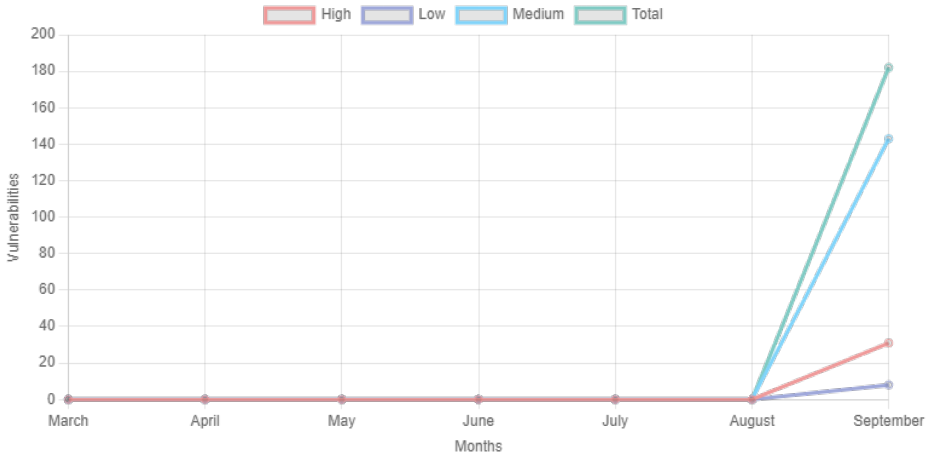
All the vulnerabilities found in your organization belong to the following categories:

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

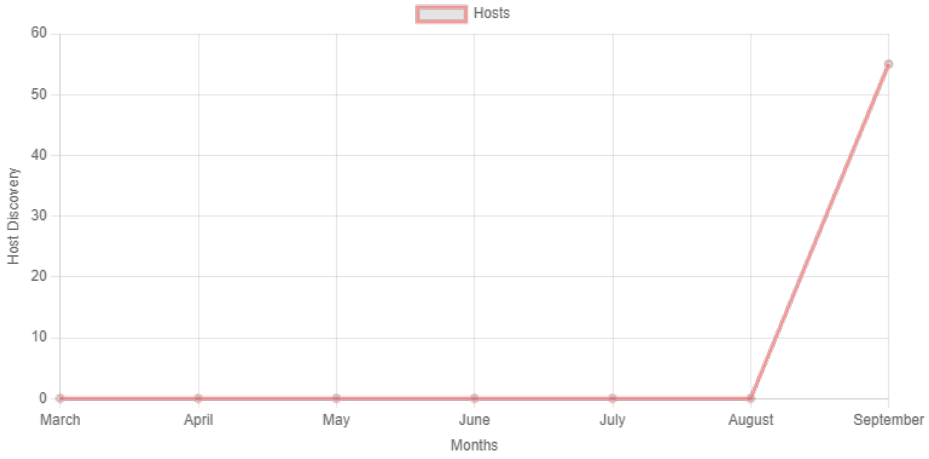
VULNERABILITY HISTOGRAM - FOR 6 MONTHS



VULNERABILITY SEVERITY HISTOGRAM - FOR 6 MONTHS



DISCOVERED NETWORK ASSET HISTOGRAM - FOR 6 MONTHS



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

COMPARISON VULNERABILITIES

	host-ip	Previous Month	Current Month
1	10.100.1.185	3	
2	10.100.1.234	5	
3	10.100.129.14	3	
4	10.100.129.143	5	
5	10.4.0.51	1	
6	172.28.1.65	2	
7	172.28.1.68	1	
8	172.28.1.70	5	
9	172.28.1.85	2	
10	172.28.1.89	4	
11	172.28.1.93	7	
12	172.28.2.108	12	
13	172.28.2.109	12	
14	172.28.2.113	12	
15	172.28.2.65	2	
16	172.28.2.75	1	
17	172.28.2.76	1	
18	172.28.2.79	1	
19	172.28.2.86	5	
20	172.28.2.97	1	
21	172.28.2.98	6	
22	192.168.100.173	3	
23	192.168.50.114	6	
24	192.168.51.15	6	
25	192.168.52.48	1	

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

VULNERABILITY CATEGORY BY RISK

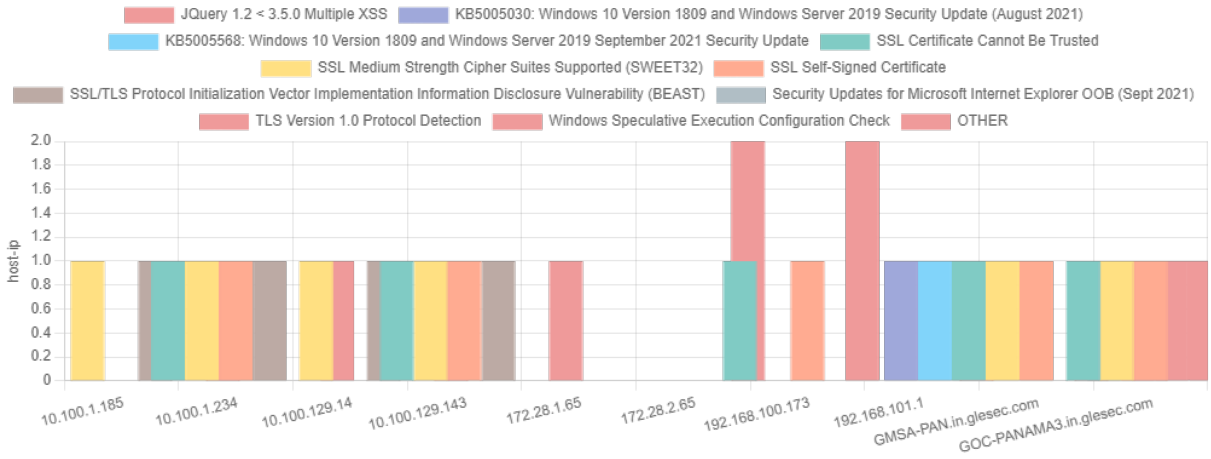
This report illustrates the vulnerability category and count by risk discovered this report period

	severity	count
1	High	21
2	Low	4
3	Medium	72

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

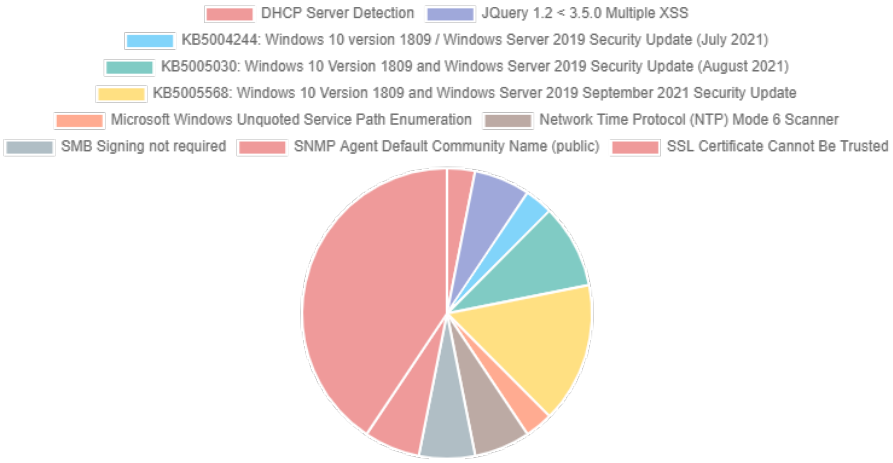
HOST BY VULNERABILITY NAME

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



MOST FREQUENT VULNERABILITY NAME

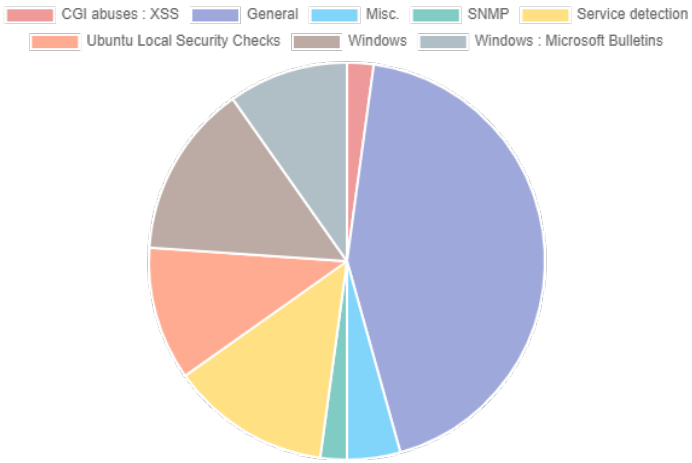
This report depicts the most frequent vulnerabilities discovered this report period



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

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

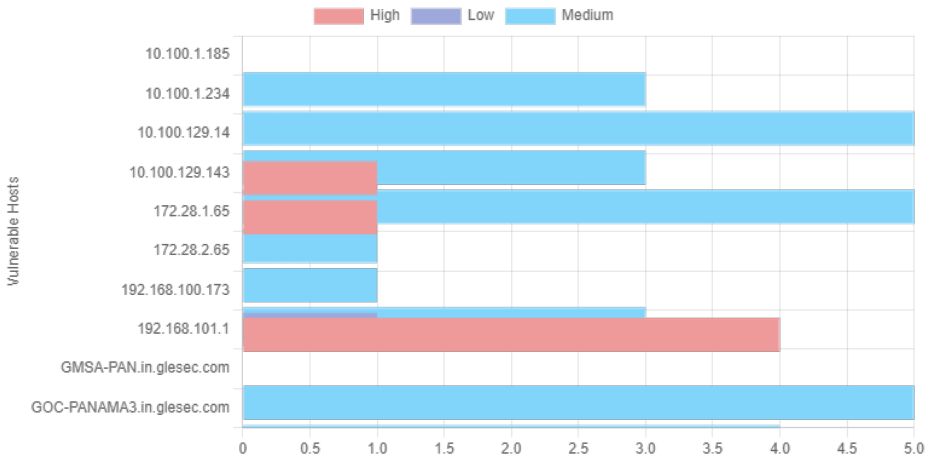
HOST BY PROTOCOL

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

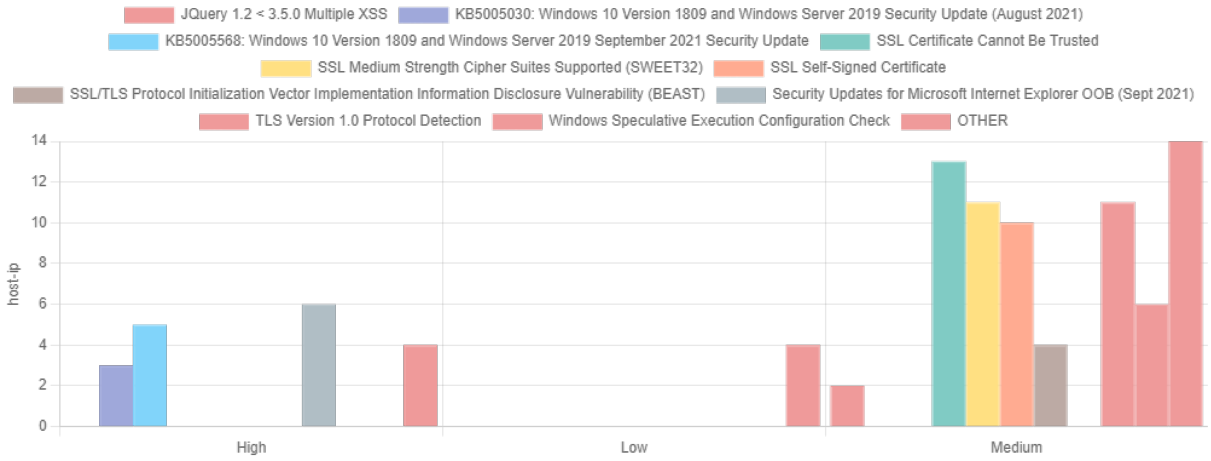
n/a

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

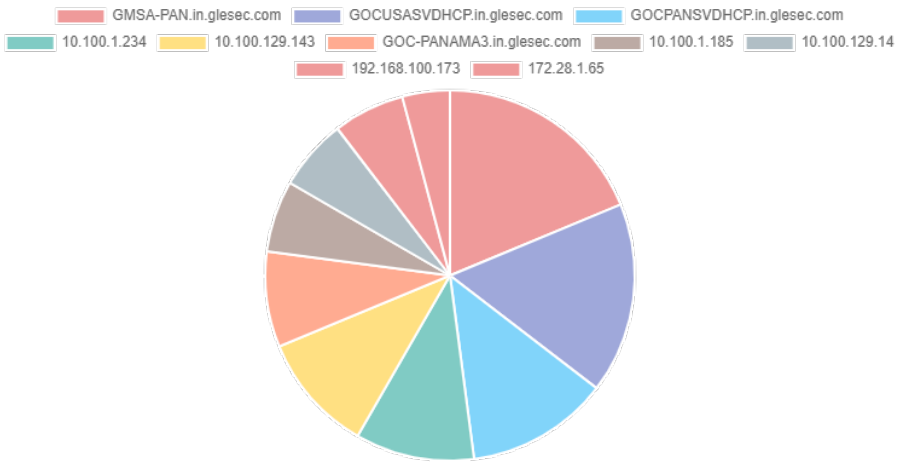
This report illustrates the vulnerability category and count by protocol discovered this report period

n/a

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

MOST VULNERABLE HOST

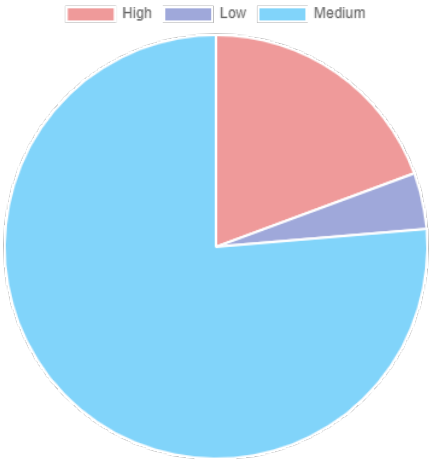
This report depicts the most vulnerable hosts discovered this report period



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

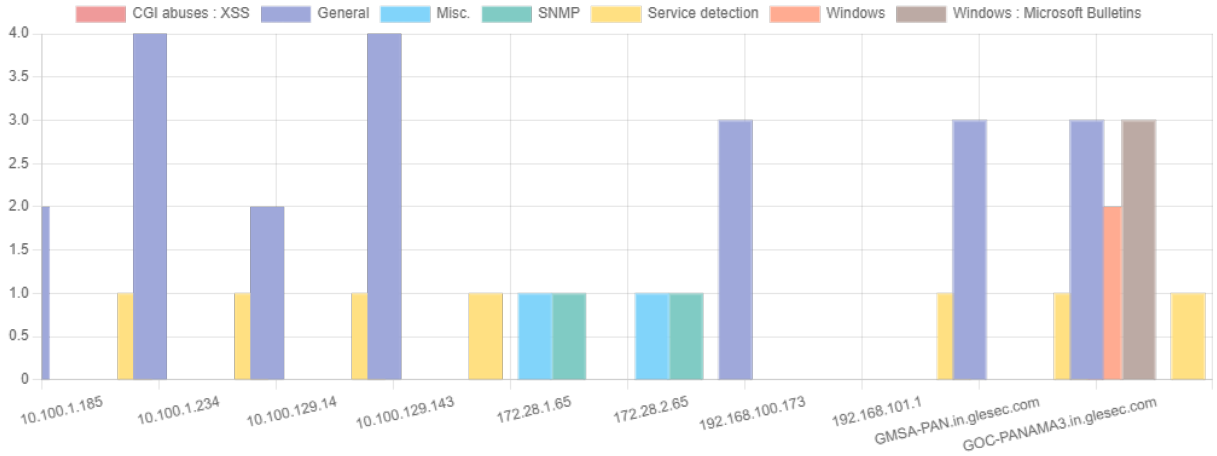
RISK DISTRIBUTION

This shows the risk distribution of vulnerabilities discovered for this period



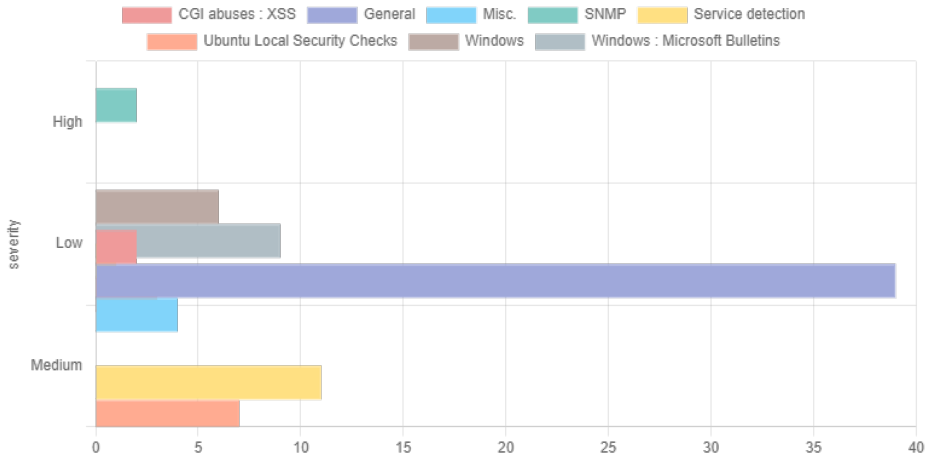
HOST BY VULNERABILITY CATEGORY

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



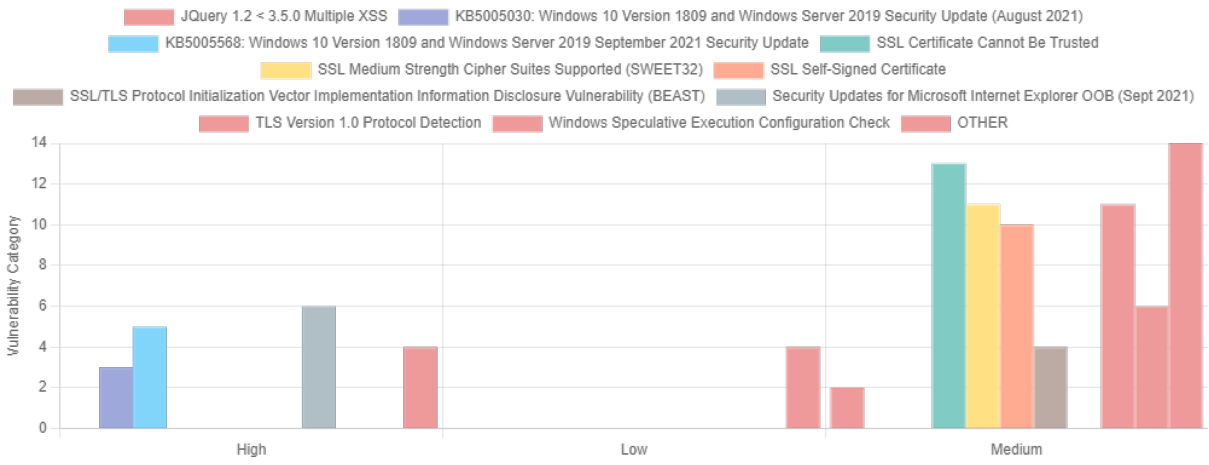
VULNERABILITY RISK BY VULNERABILITY CATEGORY

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



VULNERABILITY CATEGORY BY VULNERABILITY NAME

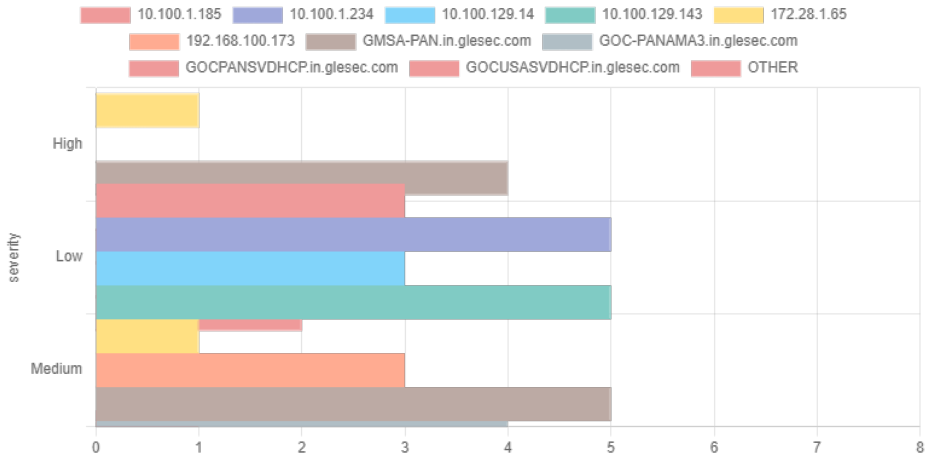
This report illustrates the vulnerability category and count by vulnerability name discovered this report period



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



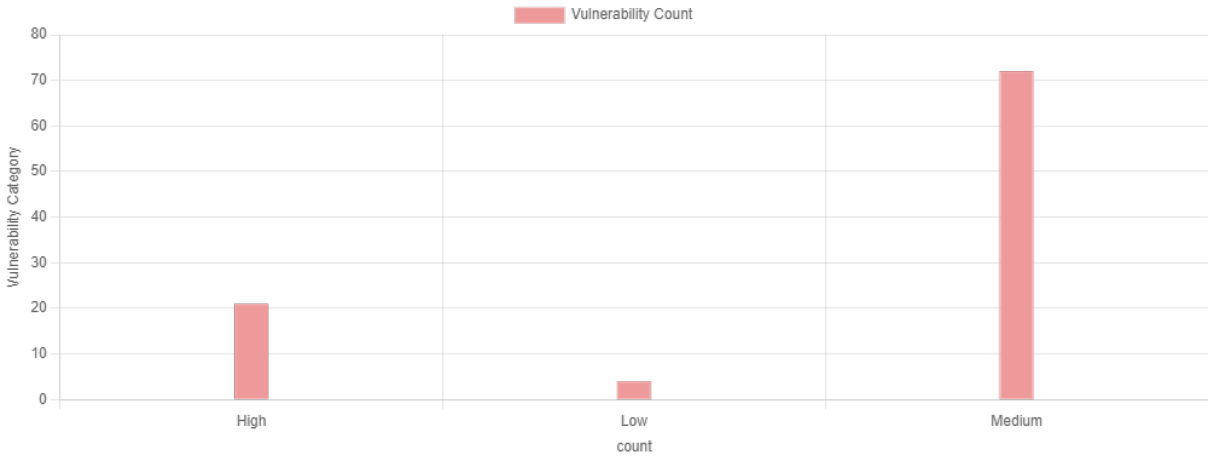
VULNERABILITY RISK BY PORT

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

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

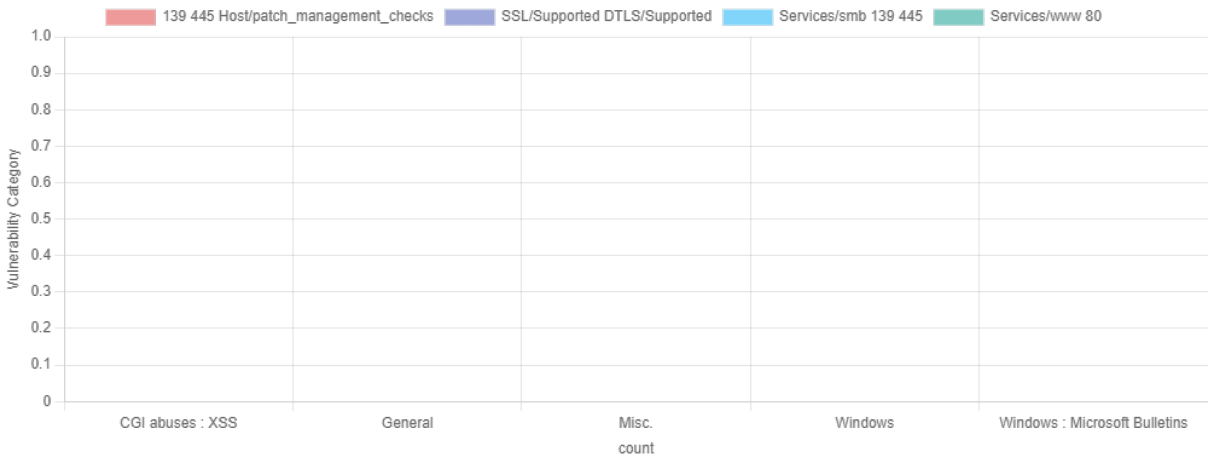
VULNERABILITY CATEGORY BY RISK

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



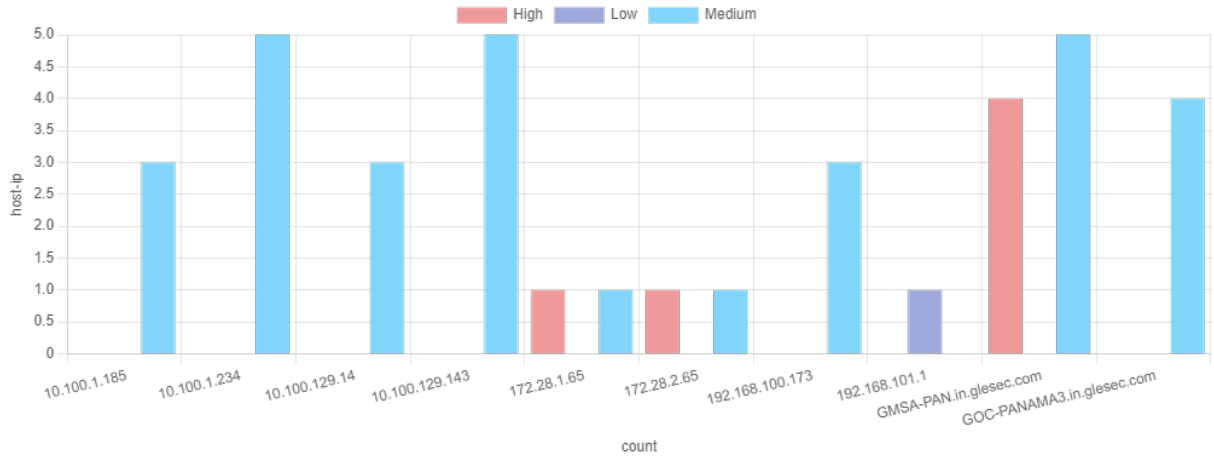
VULNERABILITY CATEGORY BY PORT

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



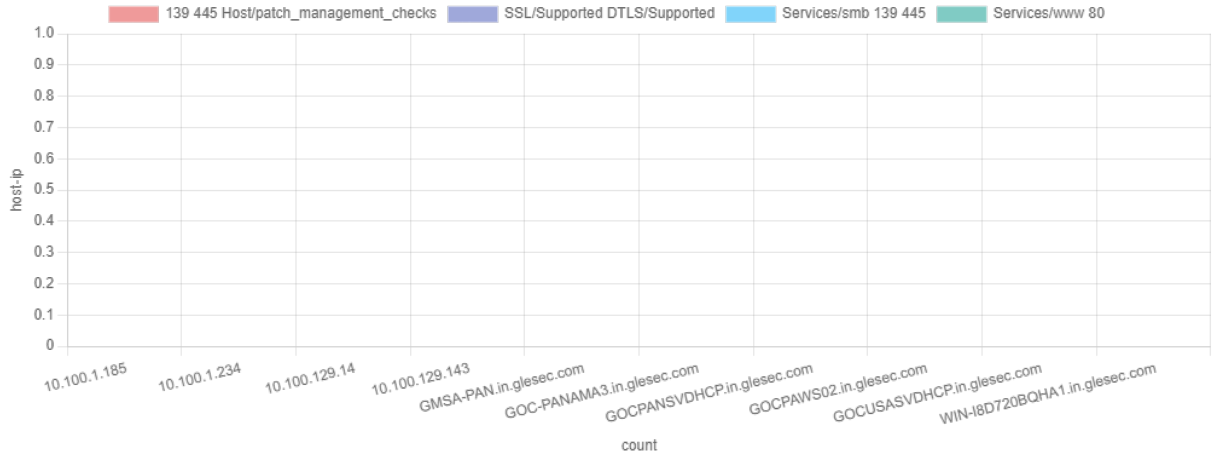
HOST BY VULNERABILITY RISK

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



VULNERABILITIES & ASSETS CORRELATION

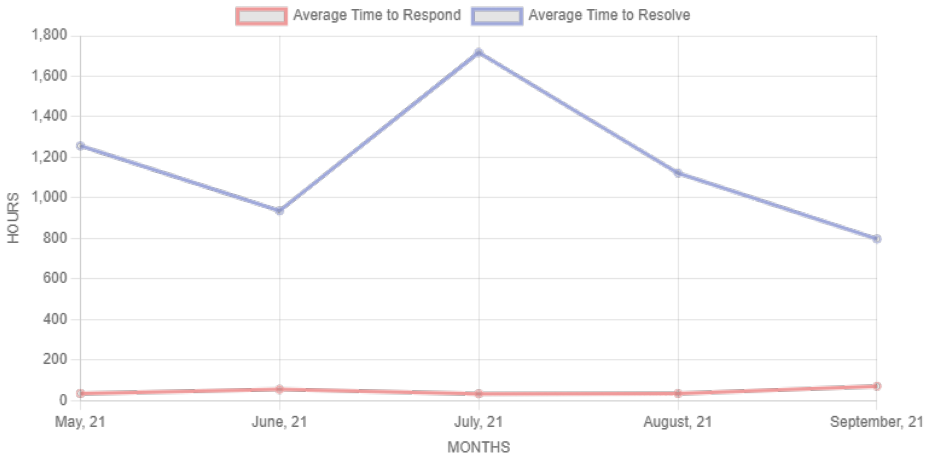
	Priority	Severity	IP	Hostname	Vulnerability	Available Exploit	Vulnerability Publication	First Seen	Days in Service	Date Scanned
1	Not Found	High			Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days			2021-09-20
2	Not Found	High			KB5005568: Windows 10 Version 1809 and Windows Server 2019 September 2021 Security Update		30 - 60 days			2021-09-20
3	Not Found	High			KB5005030: Windows 10 Version 1809 and Windows Server 2019 Security Update (August 2021)	Exploits are available	30 - 60 days			2021-09-20
4	Not Found	High			Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days			2021-09-20
5	Not Found	High			KB5005568: Windows 10 Version 1809 and Windows Server 2019 September 2021 Security Update		30 - 60 days			2021-09-20
6	Not Found	High			Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days			2021-09-20
7	Not Found	High			KB5005568: Windows 10 Version 1809 and Windows Server 2019 September 2021 Security Update		30 - 60 days			2021-09-20
8	Medium	High	172.28.2.98	GOCUSASVDHCP.in.glesec.com	Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days	2021-09-13	9	2021-09-20
9	Medium	High	172.28.2.98	GOCUSASVDHCP.in.glesec.com	KB5005568: Windows 10 Version 1809 and Windows Server 2019 September 2021 Security Update		30 - 60 days	2021-09-20	2	2021-09-20
10	Medium	High	172.28.2.98	GOCUSASVDHCP.in.glesec.com	KB5005030: Windows 10 Version 1809 and Windows Server 2019 Security Update (August 2021)	Exploits are available	30 - 60 days	2021-09-13	9	2021-09-20
11	Medium	High	172.28.2.89	goc-usa-sw.in.glesec.com	TCP/IP Initial Sequence Number (ISN) Reuse Weakness	Exploits are available	730 days +	2021-09-20	2	2021-09-20
12	Medium	High	172.28.2.65		SNMP Agent Default Community Name (public)	No exploit is required	730 days +	2021-09-13	9	2021-09-20
13	Not Found	High		GMSA-PAN.in.glesec.com	Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days			2021-09-20
14	Not Found	High		GMSA-PAN.in.glesec.com	KB5005568: Windows 10 Version 1809 and Windows Server 2019 September 2021 Security Update		30 - 60 days			2021-09-20
15	Not Found	High		GMSA-PAN.in.glesec.com	KB5005030: Windows 10 Version 1809 and Windows Server 2019 Security Update (August 2021)	Exploits are available	30 - 60 days			2021-09-20
16	Not Found	High		GMSA-PAN.in.glesec.com	KB5004244: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2021)	Exploits are available	60 - 180 days			2021-09-20
17	Medium	High	172.28.1.70	GOCPANSVDHCP.in.glesec.com	Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days	2021-09-13	9	2021-09-20
18	Medium	High	172.28.1.65		SNMP Agent Default Community Name (public)	No exploit is required	730 days +	2021-09-13	9	2021-09-20
19	Not Found	High			Ubuntu 16.04 LTS : LZ4 vulnerability (USN-4968-2)	No known exploits are available	60 - 180 days			2021-09-13
20	Not Found	High			Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days			2021-09-13
21	Not Found	High			KB5005030: Windows 10 Version 1809 and Windows Server 2019 Security Update (August 2021)	Exploits are available	30 - 60 days			2021-09-13
22	Not Found	High			Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days			2021-09-13
23	Not Found	High			Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days			2021-09-13
24	Medium	High	172.28.2.98	GOCUSASVDHCP.in.glesec.com	Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days	2021-09-13	9	2021-09-13
25	Medium	High	172.28.2.98	GOCUSASVDHCP.in.glesec.com	KB5005030: Windows 10 Version 1809 and Windows Server 2019 Security Update (August 2021)	Exploits are available	30 - 60 days	2021-09-13	9	2021-09-13
26	Medium	High	172.28.2.65		SNMP Agent Default Community Name (public)	No exploit is required	730 days +	2021-09-13	9	2021-09-13
27	Not Found	High			Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days			2021-09-13
28	Not Found	High			KB5005030: Windows 10 Version 1809 and Windows Server 2019 Security Update (August 2021)	Exploits are available	30 - 60 days			2021-09-13
29	Not Found	High			KB5004244: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2021)	Exploits are available	60 - 180 days			2021-09-13
30	Medium	High	172.28.1.70	GOCPANSVDHCP.in.glesec.com	Security Updates for Microsoft Internet Explorer OOB (Sept 2021)	Exploits are available	0 - 7 days	2021-09-13	9	2021-09-13
31	Medium	High	172.28.1.65		SNMP Agent Default Community Name (public)	No exploit is required	730 days +	2021-09-13	9	2021-09-13
32	Not Found	Medium	10.4.0.51	gmp.glesec.com	JQuery 1.2 < 3.5.0 Multiple XSS	Exploits are available	365 - 730 days	2021-09-13	9	2021-09-22
33	Not Found	Medium			Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5050-1)	No known exploits are available	30 - 60 days			2021-09-20
34	Medium	Medium	192.168.100.173		SSL Self-Signed Certificate			2021-09-13	9	2021-09-20
35	Medium	Medium	192.168.100.173		SSL Certificate Signed Using Weak Hashing Algorithm	Exploits are available	730 days +	2021-09-13	9	2021-09-20
36	Medium	Medium	192.168.100.173		SSL Certificate Cannot Be Trusted			2021-09-13	9	2021-09-20
37	Not Found	Medium			SSL Certificate Cannot Be Trusted					2021-09-20
38	Not Found	Medium			Ubuntu 16.04 LTS : systemd vulnerabilities (USN-5013-2)	Exploits are available	30 - 60 days			2021-09-20
39	Not Found	Medium			Ubuntu 16.04 LTS : Squashfs-Tools vulnerabilities (USN-5078-2)	No known exploits are available	7 - 30 days			2021-09-20
40	Not Found	Medium			Ubuntu 16.04 LTS : Python vulnerabilities (USN-5083-1)	No known exploits are available				2021-09-20
41	Not Found	Medium			Ubuntu 16.04 LTS : OpenSSL vulnerability (USN-5051-2)	No known exploits are available	7 - 30 days			2021-09-20
42	Not Found	Medium			Ubuntu 16.04 LTS : Linux kernel vulnerability (USN-5039-1)	Exploits are available	60 - 180 days			2021-09-20
43	Not Found	Medium			Ubuntu 16.04 LTS : libsndfile vulnerability (USN-5025-2)	No known exploits are available	30 - 60 days			2021-09-20
44	Not Found	Medium			Ubuntu 16.04 LTS : curl vulnerabilities (USN-5079-2)	No known exploits are available				2021-09-20
45	Not Found	Medium			Windows Speculative Execution Configuration Check	Exploits are available	730 days +			2021-09-20
46	Not Found	Medium			TLS Version 1.0 Protocol Detection					2021-09-20
47	Not Found	Medium			SSL Self-Signed Certificate					2021-09-20
48	Not Found	Medium			SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +			2021-09-20
49	Not Found	Medium			SSL Certificate Cannot Be Trusted					2021-09-20
50	Not Found	Medium			Windows Speculative Execution Configuration Check	Exploits are available	730 days +			2021-09-20
51	Not Found	Medium			TLS Version 1.0 Protocol Detection					2021-09-20
52	Not Found	Medium			SSL Self-Signed Certificate					2021-09-20
53	Not Found	Medium			SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +			2021-09-20
54	Not Found	Medium			SSL Certificate Cannot Be Trusted					2021-09-20
55	Not Found	Medium			Windows Speculative Execution Configuration Check	Exploits are available	730 days +			2021-09-20
56	Not Found	Medium			TLS Version 1.0 Protocol Detection					2021-09-20
57	Not Found	Medium			SSL Self-Signed Certificate					2021-09-20
58	Not Found	Medium			SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +			2021-09-20
59	Not Found	Medium			SSL Certificate Cannot Be Trusted					2021-09-20
60	Medium	Medium	172.28.2.98	GOCUSASVDHCP.in.glesec.com	Windows Speculative Execution Configuration Check	Exploits are available	730 days +	2021-09-13	9	2021-09-20
61	Medium	Medium	172.28.2.98	GOCUSASVDHCP.in.glesec.com	TLS Version 1.0 Protocol Detection			2021-09-13	9	2021-09-20
62	Medium	Medium	172.28.2.98	GOCUSASVDHCP.in.glesec.com	SSL Self-Signed Certificate			2021-09-13	9	2021-09-20
63	Medium	Medium	172.28.2.98	GOCUSASVDHCP.in.glesec.com	SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +	2021-09-13	9	2021-09-20
64	Medium	Medium	172.28.2.98	GOCUSASVDHCP.in.glesec.com	SSL Certificate Cannot Be Trusted			2021-09-13	9	2021-09-20
65	Medium	Medium	172.28.2.97	GOCUSAWS03.in.glesec.com	Microsoft Windows Unquoted Service Path Enumeration	Exploits are available	730 days +	2021-09-13	9	2021-09-20
66	Not Found	Medium	172.28.2.80	WIN-I8D720BQHA1.in.glesec.com	SMB Signing not required	Exploits are available		2021-09-20	2	2021-09-20
67	Medium	Medium	172.28.2.76	SIP-T23G.in.glesec.com	SSL Certificate Cannot Be Trusted			2021-09-13	9	2021-09-20
68	Medium	Medium	172.28.2.75	SIP-T23G.in.glesec.com	SSL Certificate Cannot Be Trusted			2021-09-13	9	2021-09-20
69	Medium	Medium	172.28.2.65		Network Time Protocol (NTP) Mode 6 Scanner			2021-09-13	9	2021-09-20
70	Not Found	Medium		GMSA-PAN.in.glesec.com	Windows Speculative Execution Configuration Check	Exploits are available	730 days +			2021-09-20
71	Not Found	Medium		GMSA-PAN.in.glesec.com	TLS Version 1.0 Protocol Detection					2021-09-20
72	Not Found	Medium		GMSA-PAN.in.glesec.com	SSL Self-Signed Certificate					2021-09-20
73	Not Found	Medium		GMSA-PAN.in.glesec.com	SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +			2021-09-20
74	Not Found	Medium		GMSA-PAN.in.glesec.com	SSL Certificate Cannot Be Trusted					2021-09-20
75	Medium	Medium	172.28.1.89	GOC-PANAMA3.in.glesec.com	TLS Version 1.0 Protocol Detection			2021-09-13	9	2021-09-20
76	Medium	Medium	172.28.1.89	GOC-PANAMA3.in.glesec.com	SSL Self-Signed Certificate			2021-09-13	9	2021-09-20
77	Medium	Medium	172.28.1.89	GOC-PANAMA3.in.glesec.com	SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +	2021-09-13	9	2021-09-20
78	Medium	Medium	172.28.1.89	GOC-PANAMA3.in.glesec.com	SSL Certificate Cannot Be Trusted			2021-09-13	9	2021-09-20
79	Medium	Medium	172.28.1.70	GOCPANSVDHCP.in.glesec.com	Windows Speculative Execution Configuration Check	Exploits are available	730 days +	2021-09-13	9	2021-09-20
80	Medium	Medium	172.28.1.70	GOCPANSVDHCP.in.glesec.com	TLS Version 1.0 Protocol Detection			2021-09-13	9	2021-09-20
81	Medium	Medium	172.28.1.70	GOCPANSVDHCP.in.glesec.com	SSL Self-Signed Certificate			2021-09-13	9	2021-09-20
82	Medium	Medium	172.28.1.70	GOCPANSVDHCP.in.glesec.com	SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +	2021-09-13	9	2021-09-20
83	Medium	Medium	172.28.1.70	GOCPANSVDHCP.in.glesec.com	SSL Certificate Cannot Be Trusted			2021-09-13	9	2021-09-20
84	Medium	Medium	172.28.1.68	GOCPAWS02.in.glesec.com	SMB Signing not required	Exploits are available		2021-09-13	9	2021-09-20
85	Medium	Medium	172.28.1.65		Network Time Protocol (NTP) Mode 6 Scanner			2021-09-13	9	2021-09-20
86	Not Found	Medium	10.100.129.143		TLS Version 1.0 Protocol Detection			2021-09-13	9	2021-09-20
87	Not Found	Medium	10.100.129.143		SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	No known exploits are available	730 days +	2021-09-13	9	2021-09-20
88	Not Found	Medium	10.100.129.143		SSL Self-Signed Certificate			2021-09-13	9	2021-09-20
89	Not Found	Medium	10.100.129.143		SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +	2021-09-13	9	2021-09-20
90	Not Found	Medium	10.100.129.143		SSL Certificate Cannot Be Trusted			2021-09-13	9	2021-09-20
91	Not Found	Medium	10.100.129.14		TLS Version 1.0 Protocol Detection			2021-09-13	9	2021-09-20
92	Not Found	Medium	10.100.129.14		SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	No known exploits are available	730 days +	2021-09-13	9	2021-09-20
93	Not Found	Medium	10.100.129.14		SSL Medium Strength Cipher Suites Supported (SWEET32)		730 days +	2021-09-13	9	2021-09-20
94	Not Found	Medium	10.100.1.234		TLS Version 1.0 Protocol Detection			2021-09-13	9	2021-09-20
95	Not Found	Medium	10.100.1.234		SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	No known exploits are available	730 days +	2021-09-13	9	2021-09-20

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



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).

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

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