Your Global Cyber-Security Partner

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

TLP-AMBER

GLESEC

December 5, 2022

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

About This Report

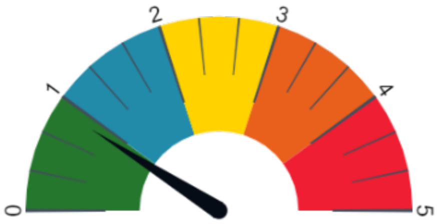
This on-demand technical report is compiled for the people with responsibility for Cyber Security, Networking, Databases, Compliance, Infrastructure and Systems. A more detail monthly report is prepared and available from the Orchestration platform (GMP). For any questions about this report please contact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

51

TOTAL VULNERABLE HOSTS

28

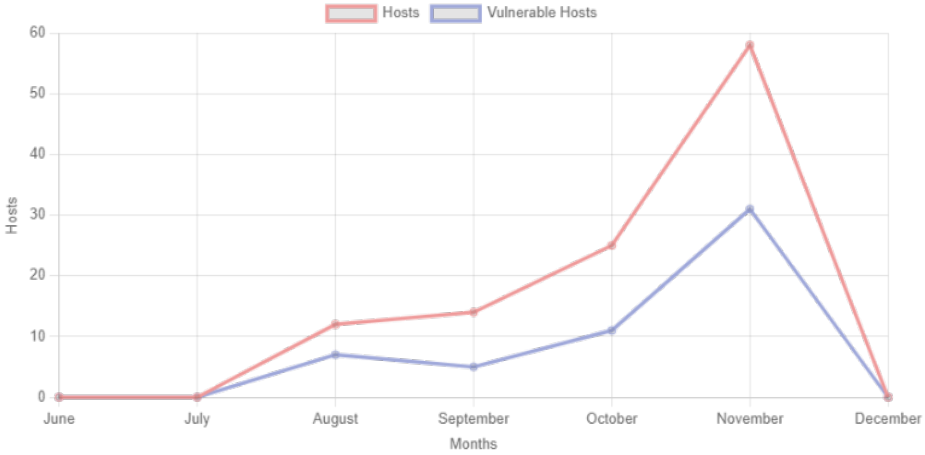
EXECUTIVE SUMMARY RISK DISTRIBUTION

Scanner	critical	high	medium	low	Total
GLESEC	8	81	184	8	281

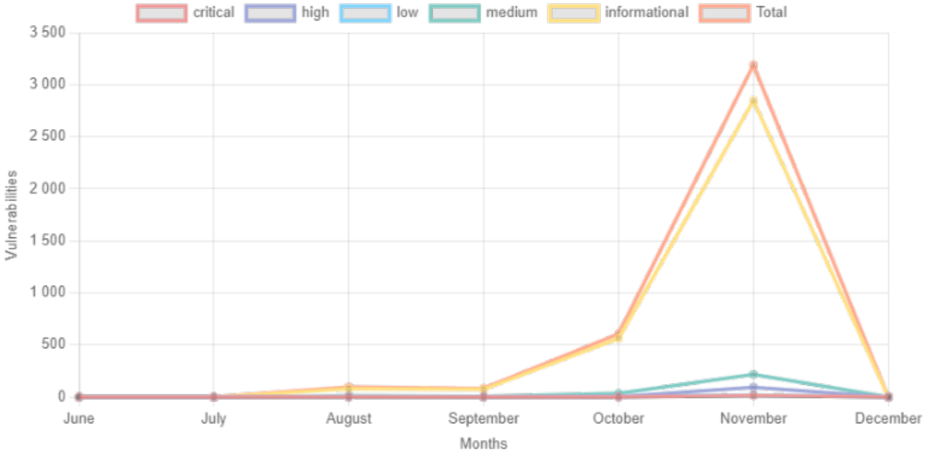
All the vulnerabilities found in your organization belong to the following categories:

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

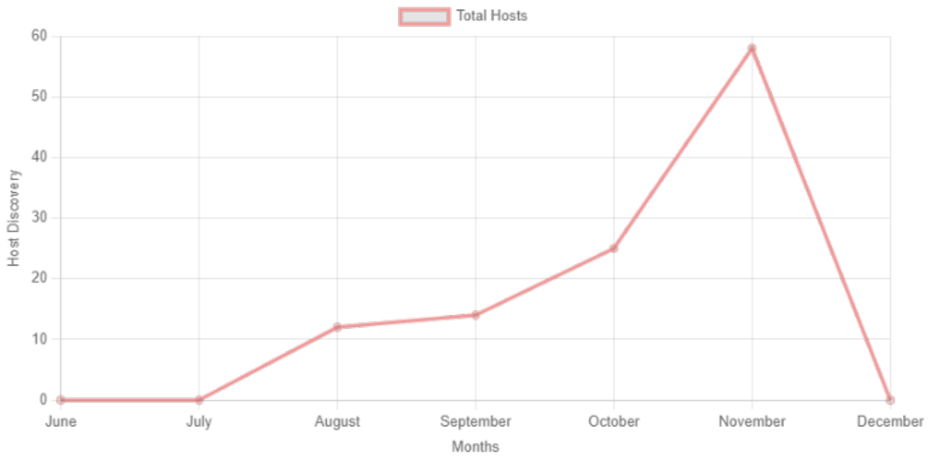
VULNERABILITY HISTOGRAM - FOR 6 MONTHS



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

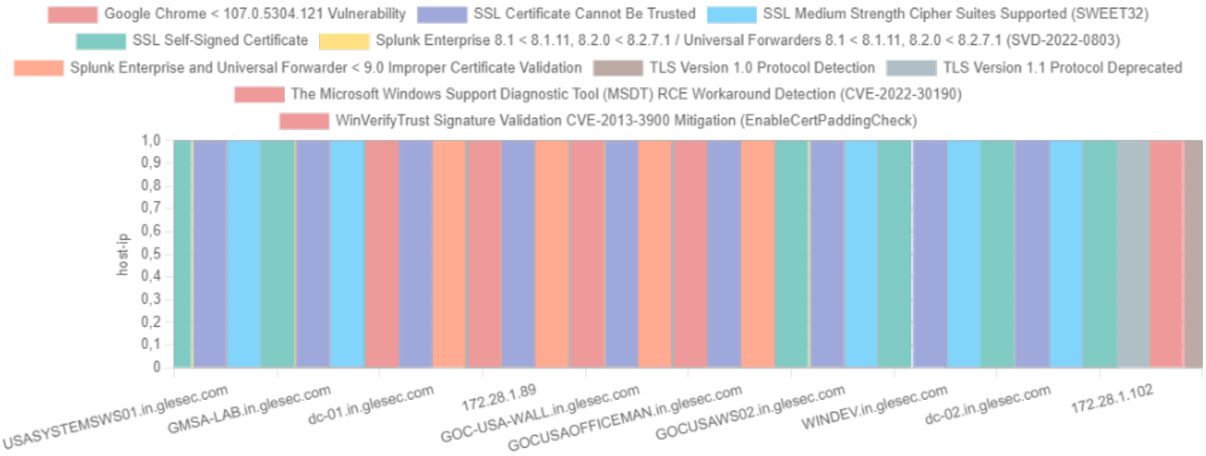
VULNERABILITY CATEGORY BY RISK

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

category	critical	high	low	medium
Windows	6	61	4	49
Misc.	0	7	0	44
General	0	1	0	48
Service detection	0	0	1	21
CGI abuses	0	0	0	18
Windows : Microsoft Bulletins	0	12	0	0
Web Servers	0	0	3	0
Backdoors	2	0	0	0
CGI abuses : XSS	0	0	0	2
CISCO	0	0	0	1

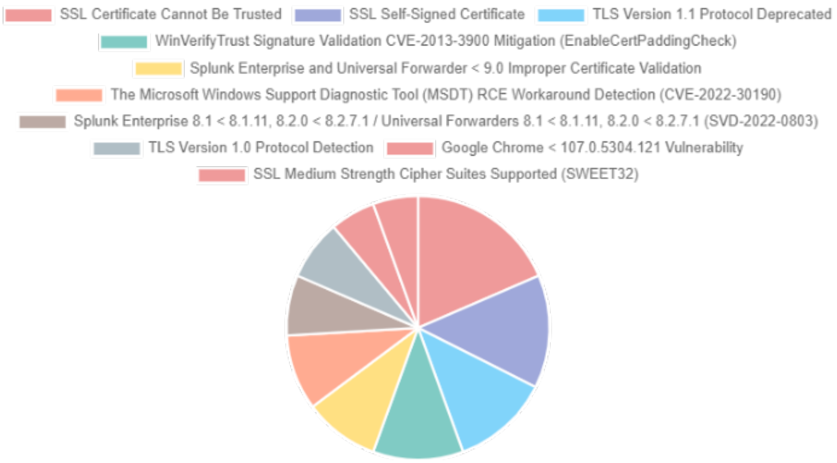
HOST BY VULNERABILITY NAME

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



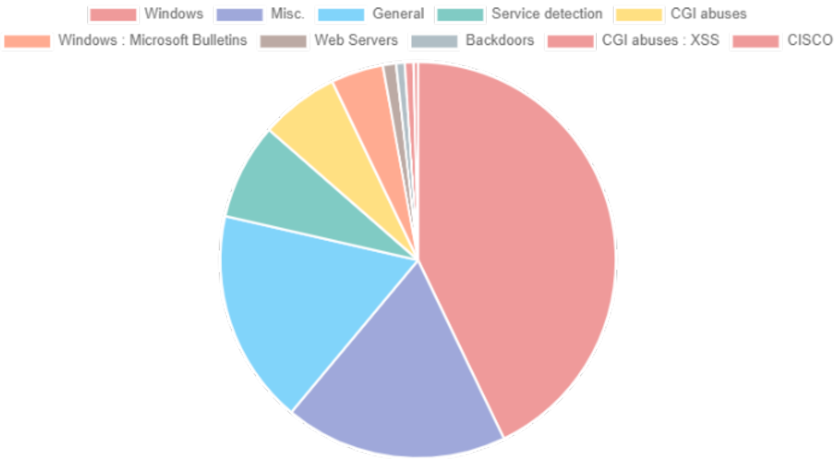
MOST FREQUENT VULNERABILITY NAME

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

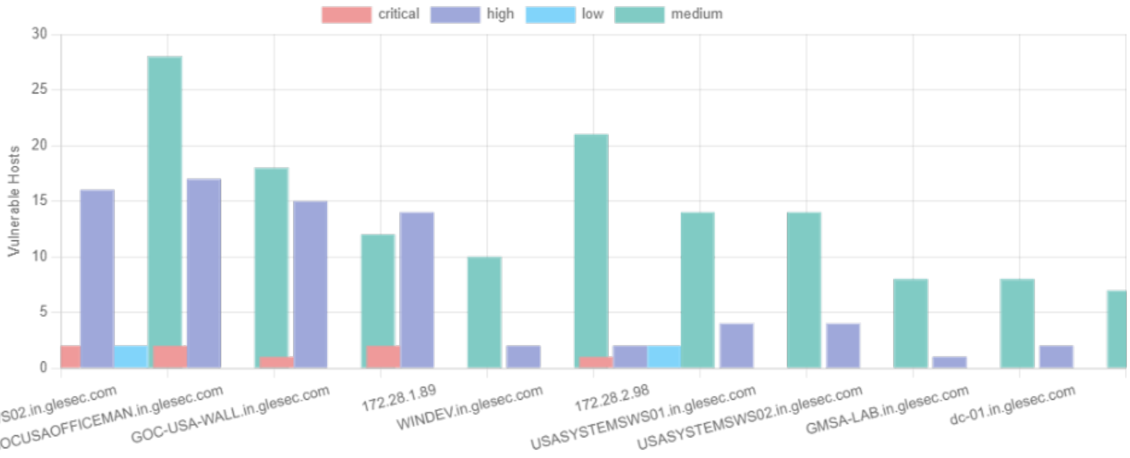
HOST BY PROTOCOL

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

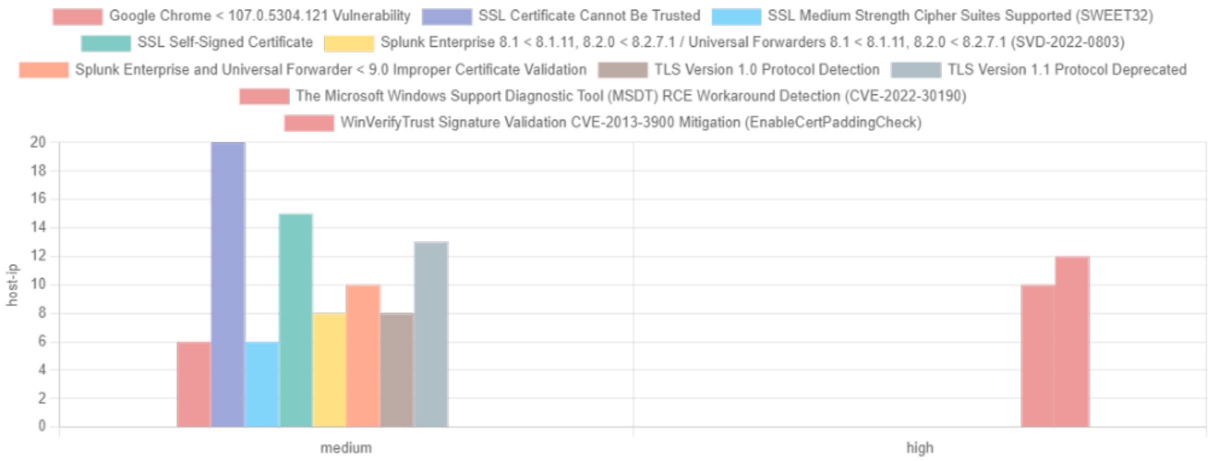
n/a

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

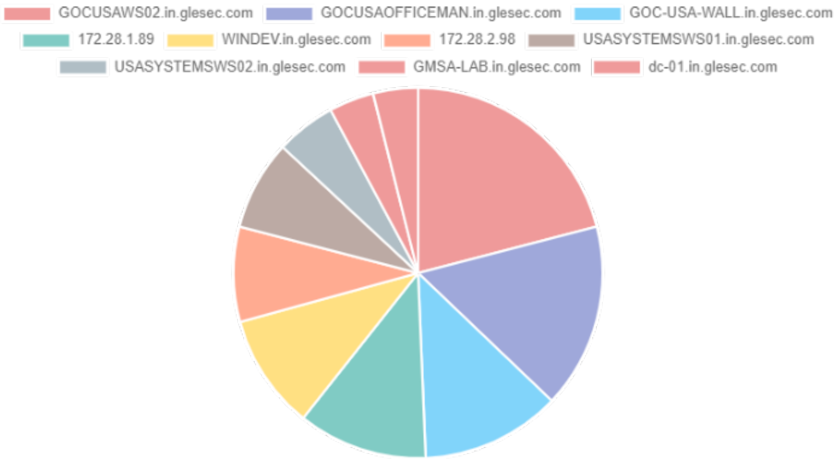
This report illustrates the vulnerability category and count by protocol discovered this report period

n/a

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

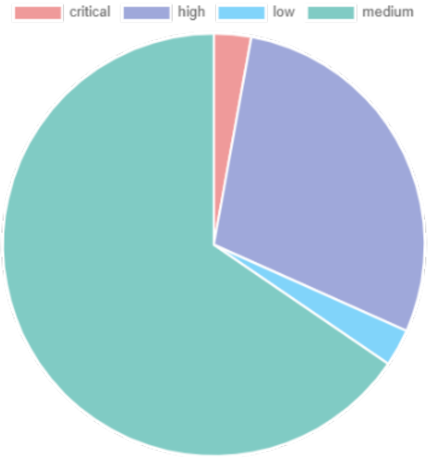
MOST VULNERABLE HOST

This report depicts the most vulnerable hosts discovered this report period



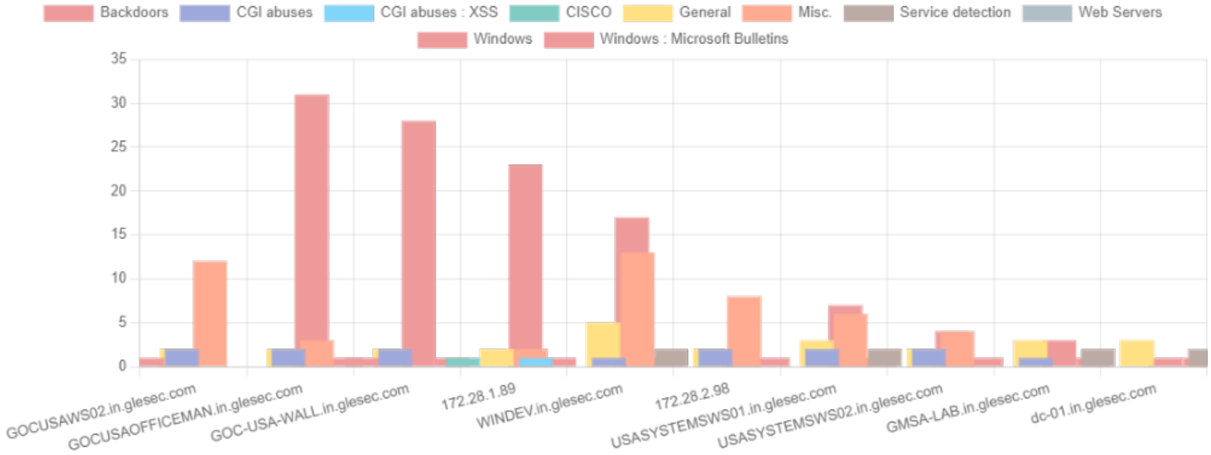
RISK DISTRIBUTION

This shows the risk distribution of vulnerabilities discovered for this period



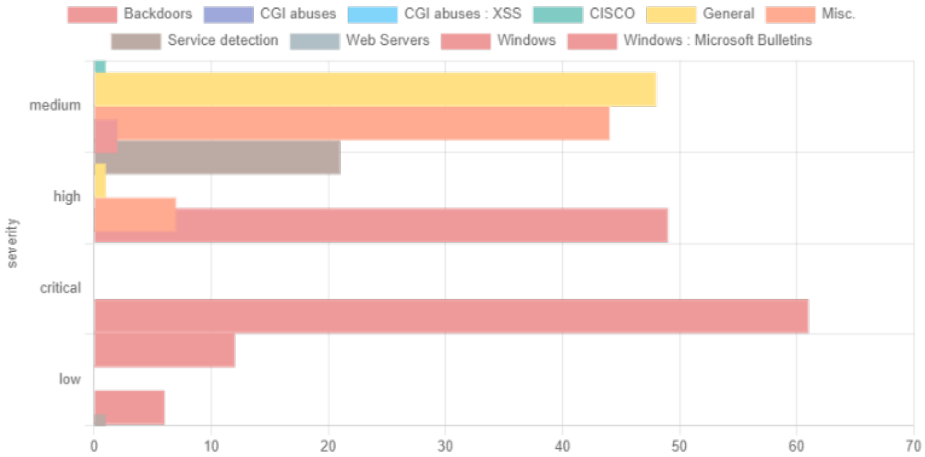
HOST BY VULNERABILITY CATEGORY

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



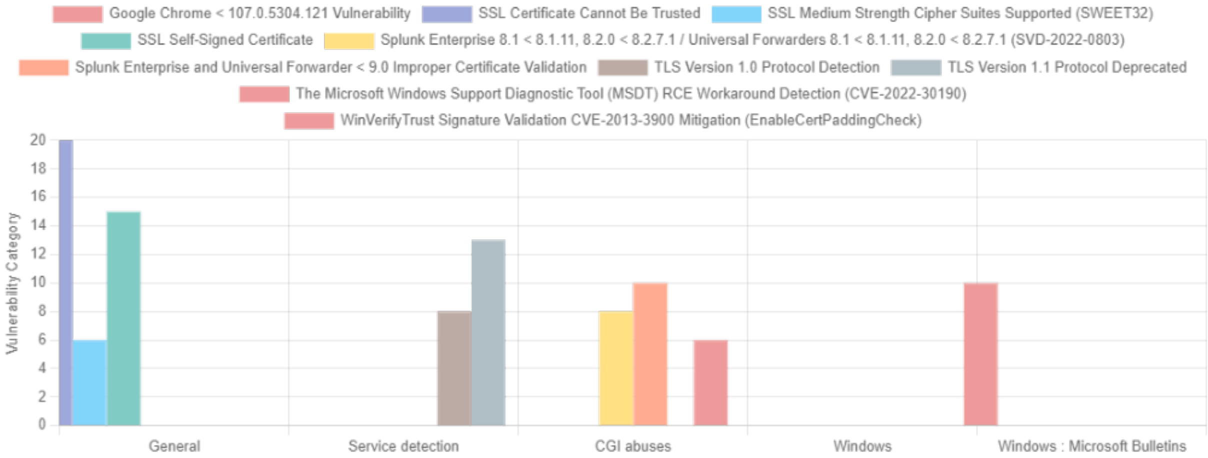
VULNERABILITY RISK BY VULNERABILITY CATEGORY

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



VULNERABILITY CATEGORY BY VULNERABILITY NAME

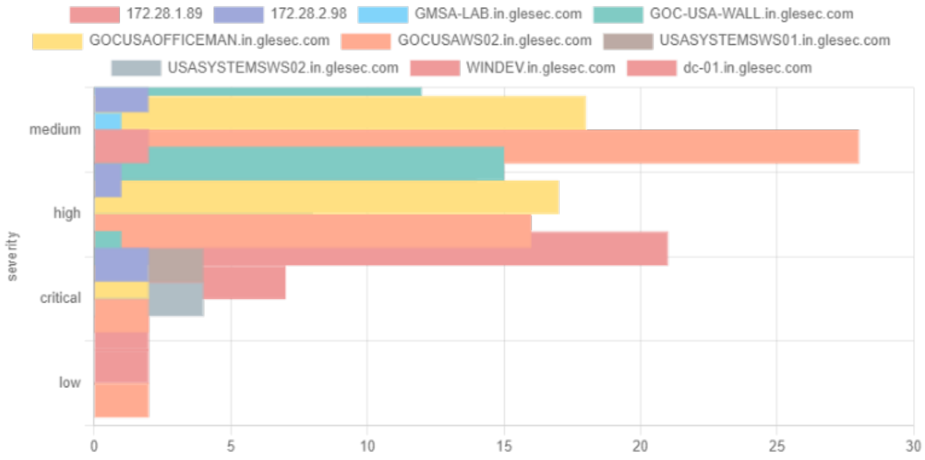
This report illustrates the vulnerability category and count by vulnerability name discovered this report period



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



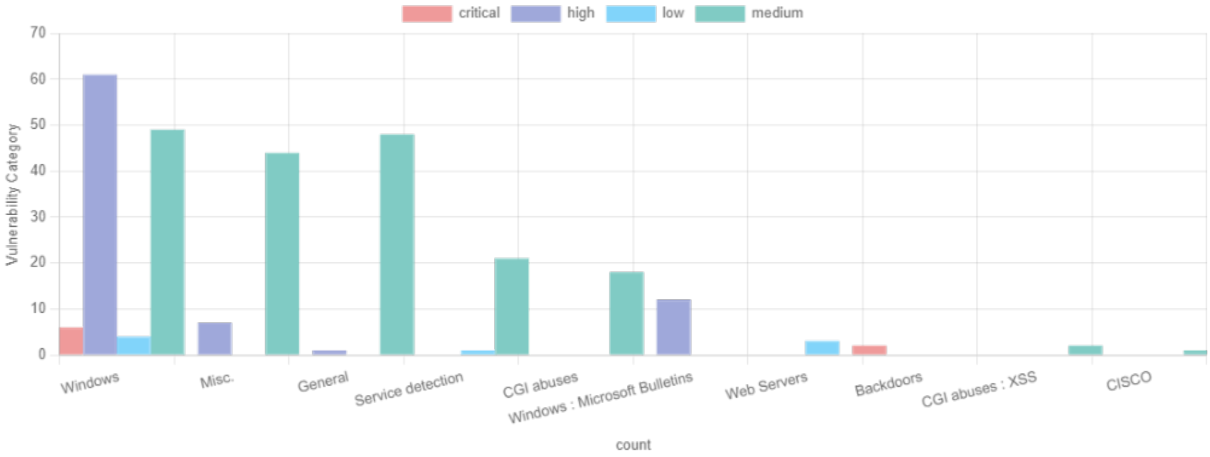
VULNERABILITY RISK BY PORT

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



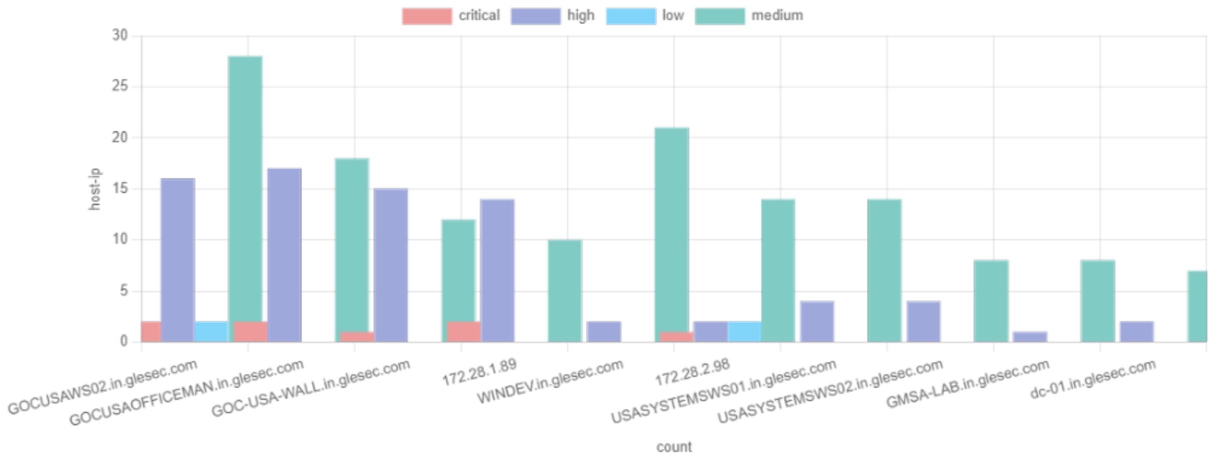
VULNERABILITY CATEGORY BY PORT

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	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	SSL Self-Signed Certificate	57582	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
Medium	Medium	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Google Chrome < 107.0.5304.121 Vulnerability	168181	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
Medium	Medium	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Intel® PROSet/Wireless WiFi Software x < 21.70.0 Multiple Vulnerabilities	136670	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
Medium	Medium	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Mozilla Firefox < 91.0	152412	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
Medium	Medium	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Mozilla Firefox < 99.0	159530	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
Medium	Medium	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Splunk Enterprise 8.1 < 8.1.11, 8.2.0 < 8.2.7.1 / Universal Forwarders 8.1 < 8.1.11, 8.2.0 < 8.2.7.1 (SVD-2022-0803)	164329	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
Medium	Medium	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Zoom Client < 5.10.0 Attack Chain Vulnerabilities	161760	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
Medium	Medium	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Zoom Client < 5.11.0 URL Parsing Vulnerability	165674	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
Medium	Medium	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Zoom Client < 5.9.7	161702	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
High	Critical	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Compromised Windows System (hosts File Check)	23910	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
High	Critical	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Mozilla Foundation Unsupported Application Detection	40362	n/a	n/a	07 day(s)	

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Medium	172.28.2.109	Hyper-V Server 2019	GMSA-LAB.in.glesec.com	Not Set	Not Set	Splunk Enterprise and Universal Forwarder < 9.0 Improper Certificate Validation	164078	n/a	n/a	07 day(s)	2022/11/28 10:46:13-0500
Medium	Medium	172.28.2.108	Hyper-V Server 2019	GMSA-LAB.in.glesec.com	Not Set	Not Set	Splunk Enterprise 8.1 < 8.1.11, 8.2.0 < 8.2.7.1 / Universal Forwarders 8.1 < 8.1.11, 8.2.0 < 8.2.7.1 (SVD-2022-0803)	164329	n/a	n/a	07 day(s)	2022/11/28 10:43:04-0500
Medium	Medium	172.28.2.108	Hyper-V Server 2019	GMSA-LAB.in.glesec.com	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	07 day(s)	2022/11/28 10:43:04-0500
Medium	Medium	172.28.2.124		Unknown	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	07 day(s)	2022/11/28 10:39:23-0500
Medium	Medium	192.168.51.15	Microsoft Windows Server 2019 Datacenter	dc-02.in.glesec.com	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	07 day(s)	2022/11/28 10:35:05-0500
Medium	High	192.168.50.114	Microsoft Windows Server 2019 Datacenter	dc-01.in.glesec.com	Not Set	Not Set	The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)	161691	n/a	2022/05/30	07 day(s)	2022/11/28 10:31:33-0500
Medium	High	192.168.50.114	Microsoft Windows Server 2019 Datacenter	dc-01.in.glesec.com	Not Set	Not Set	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	166555	true	2013/12/10	07 day(s)	2022/11/28 10:31:33-0500
Medium	Medium	192.168.50.114	Microsoft Windows Server 2019 Datacenter	dc-01.in.glesec.com	Not Set	Not Set	Splunk Enterprise and Universal Forwarder < 9.0 Improper Certificate Validation	164078	n/a	n/a	07 day(s)	2022/11/28 10:31:33-0500
Medium	Medium	192.168.50.114	Microsoft Windows Server 2019 Datacenter	dc-01.in.glesec.com	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	07 day(s)	2022/11/28 10:31:33-0500
Medium	Medium	192.168.50.114	Microsoft Windows Server 2019 Datacenter	dc-01.in.glesec.com	Not Set	Not Set	Windows Speculative Execution Configuration Check	132101	n/a	n/a	07 day(s)	2022/11/28 10:31:33-0500
Medium	Medium	172.28.2.92		Unknown	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	07 day(s)	2022/11/28 10:27:20-0500
Medium	Medium	172.28.2.89		goc-usa-sw.in.glesec.com	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	07 day(s)	2022/11/28 10:26:51-0500
Medium	Medium	172.28.2.65	FreeBSD 12.3-STABLE (arm)	Unknown	Not Set	Not Set	Network Time Protocol (NTP) Mode 6 Scanner	97861	n/a	n/a	07 day(s)	2022/11/28 09:48:13-0500
High	High	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Mozilla Firefox < 98.0	158694	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500
High	High	172.28.2.94	Microsoft Windows 10 Pro	GOCUSAOFFICEMAN.in.glesec.com	Not Set	Not Set	Zoom Client < 5.8.4 Multiple Vulnerabilities	158168	n/a	n/a	07 day(s)	2022/11/28 11:53:10-0500

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Medium	10.100.1.185	Palo Alto Networks PAN-OS	Unknown	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	07 day(s)	2022/11/28 13:17:55-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Mozilla Firefox < 100.0	160465	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Mozilla Firefox < 100.0.2	161415	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Mozilla Firefox < 101.0	161716	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Mozilla Firefox < 103.0	163497	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Mozilla Firefox < 104.0	164344	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Mozilla Firefox < 105.0	165262	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Mozilla Firefox < 106.0	166209	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Mozilla Firefox < 107.0	167633	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)	161691	n/a	2022/05/30	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	166555	true	2013/12/10	07 day(s)	2022/11/28 12:53:12-0500
Medium	Medium	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Cisco Webex Meetings App Character Interface Manipulation (cisco-sa-webex-app-qrtO6YC2)	164904	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	Medium	172.28.1.89	Microsoft Windows 10 Pro	Unknown	Not Set	Not Set	Splunk Enterprise and Universal Forwarder < 9.0 Improper Certificate Validation	164078	n/a	n/a	07 day(s)	2022/11/28 12:53:12-0500
Medium	High	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)	161691	n/a	2022/05/30	07 day(s)	2022/11/28 12:51:35-0500
Medium	High	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	166555	true	2013/12/10	07 day(s)	2022/11/28 12:51:35-0500

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	OpenJDK 7 <= 7u331 / 8 <= 8u322 / 11.0.0 <= 11.0.14 / 13.0.0 <= 13.0.10 / 15.0.0 <= 15.0.6 / 17.0.0 <= 17.0.2 / 18.0.0 <= 18.0.0 Multiple Vulnerabilities (2022-04-19)	159948	false	2022/04/17	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	OpenJDK 7 <= 7u341 / 8 <= 8u332 / 11.0.0 <= 11.0.15 / 13.0.0 <= 13.0.11 / 15.0.0 <= 15.0.7 / 17.0.0 <= 17.0.3 / 18.0.0 <= 18.0.1 Multiple Vulnerabilities (2022-07-19	163455	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	SSL Certificate Cannot Be Trusted	51192	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	SSL Medium Strength Cipher Suites Supported (SWEET32)	42873	n/a	2016/08/24	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	Security Update for Microsoft Visual Studio Code (April 2022)	159759	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	Security Update for Microsoft Visual Studio Code (December 2021)	156101	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	Security Update for Microsoft Visual Studio Code (February 2022)	157430	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	Security Update for Microsoft Visual Studio Code (March 2022)	158785	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	Security Update for Microsoft Visual Studio Code (May 2022)	160944	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	Security Update for Microsoft Visual Studio Code (November 2021)	154992	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	172.28.2.93	Microsoft Windows 10 Pro	WINDEV.in.glesec.com	Not Set	Not Set	SSL Certificate Expiry	15901	n/a	n/a	07 day(s)	2022/11/28 12:51:35-0500
Medium	Medium	10.100.129.14	Palo Alto Networks PAN-OS	Unknown	Not Set	Not Set	TLS Version 1.1 Protocol Deprecated	157288	n/a	n/a	07 day(s)	2022/11/28 12:18:16-0500
Medium	Medium	192.168.52.48	Linux Kernel 5.11.0-1023-aws on Ubuntu 20.04	netbox.in.glesec.com	Not Set	Not Set	Splunk Enterprise and Universal Forwarder < 9.0 Improper Certificate Validation	164078	n/a	n/a	07 day(s)	2022/11/28 10:51:30-0500
Medium	Medium	192.168.52.48	Linux Kernel 5.11.0-1023-aws on Ubuntu 20.04	netbox.in.glesec.com	Not Set	Not Set	SSL Certificate Cannot Be Trusted	51192	n/a	n/a	07 day(s)	2022/11/28 10:51:30-0500
Medium	High	172.28.2.109	Hyper-V Server 2019	GMSA-LAB.in.glesec.com	Not Set	Not Set	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	166555	true	2013/12/10	07 day(s)	2022/11/28 10:46:13-0500

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