



Your Global Cyber-Security Partner

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

GLESEC
July 22, 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

44

TOTAL VULNERABLE HOSTS

1

EXECUTIVE SUMMARY RISK DISTRIBUTION

	name	Critical	High	Medium	Low	Total
1	GLESEC			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

COMPARISON VULNERABILITIES

	host-ip	Previous Month	Current Month
1	10.4.0.51		1
2	172.28.1.94	5	
3	172.28.2.68	1	
4	172.28.2.86	5	
5	172.28.2.91	1	
6	192.168.10.103	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

	Category	Critical	High	Medium	Low	Total
1	CGI abuses : XSS			1		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

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

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

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

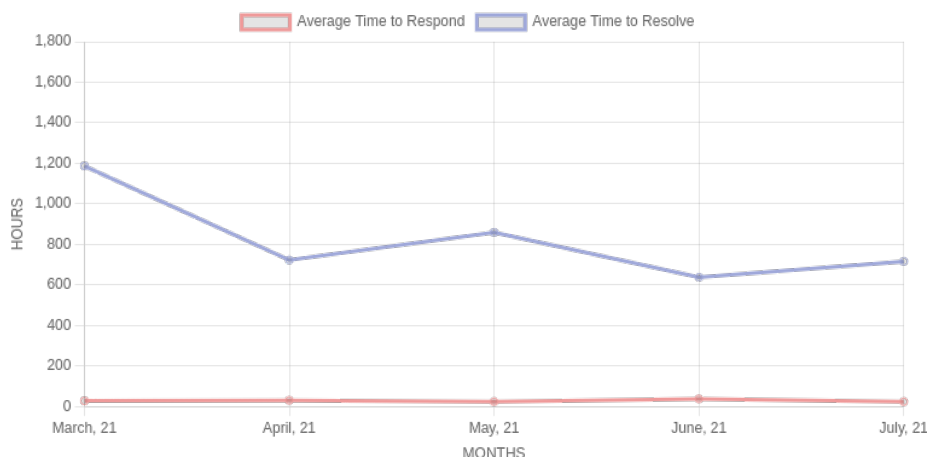
Severity	Hostname	IP	Priority	Vulnerability	Vulnerability-ID	Date Scanned
1 medium	gmp.glesec.com	10.4.0.51		JQuery 1.2 < 3.5.0 Multiple XSS	136929	2021-07-21
2 medium	mss-vme.in.glesec.com	192.168.101.65		JQuery 1.2 < 3.5.0 Multiple XSS	136929	2021-07-21
3 medium	mss-vme.in.glesec.com	192.168.101.65		Web Application Potentially Vulnerable to Clickjacking	85582	2021-07-21
4 medium		192.168.52.48		Web Application Potentially Vulnerable to Clickjacking	85582	2021-07-21

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).



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

