TLP:AMBER

MSS-IOT REPORT

GLESEC

July 12, 2024

TLP AMBER
MSS-IOT REPORT

About this report

This is a SKYWATCH report that presents the most up-to-date information for the MSS-IOT as displayed in the service dashboard.

Overview

Vulnerability Level

28%

Discovered Hosts

10

Vulnerable Hosts

6

Executive Summary Vulnerability Severity Distribution

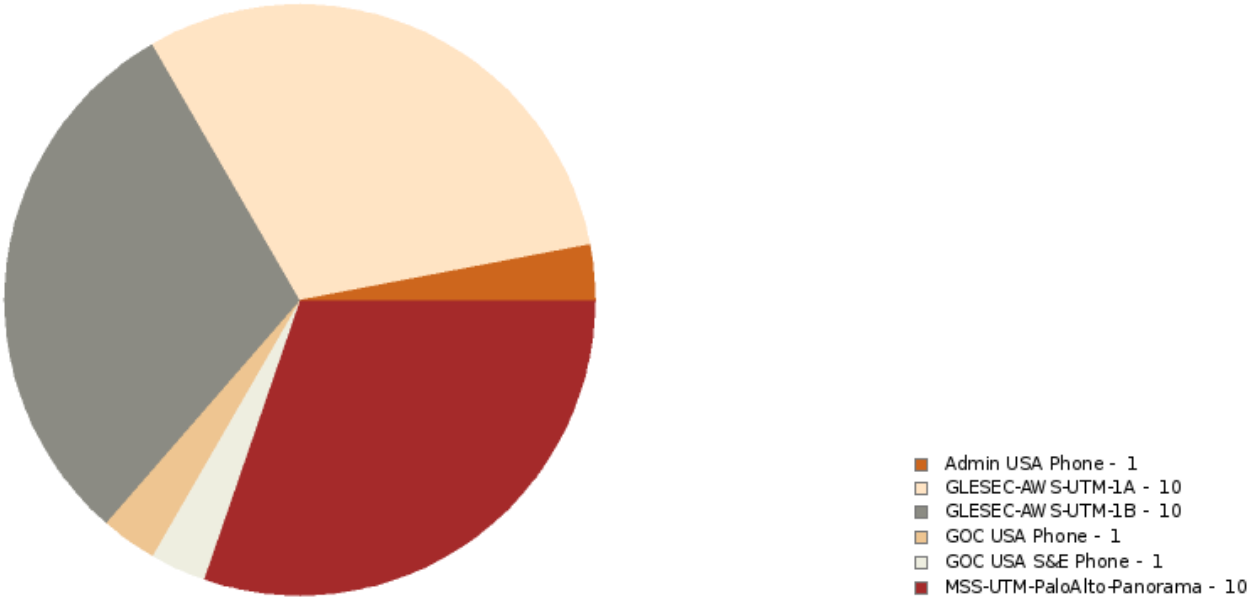
Site	critical	high	medium	low	Total
AWS	3	3	21	3	30
GOC-USA	3	0	0	0	3

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

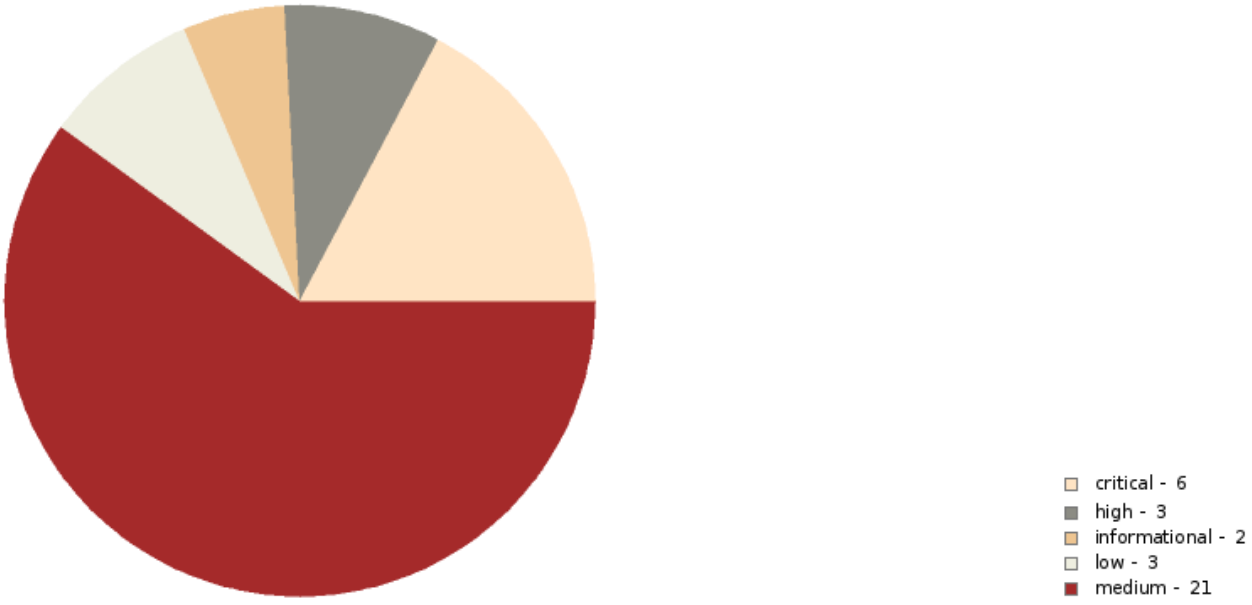
MSS-IOT REPORT

GLESEC 07/12/2024

Most Vulnerable Host *



Vulnerability Distribution



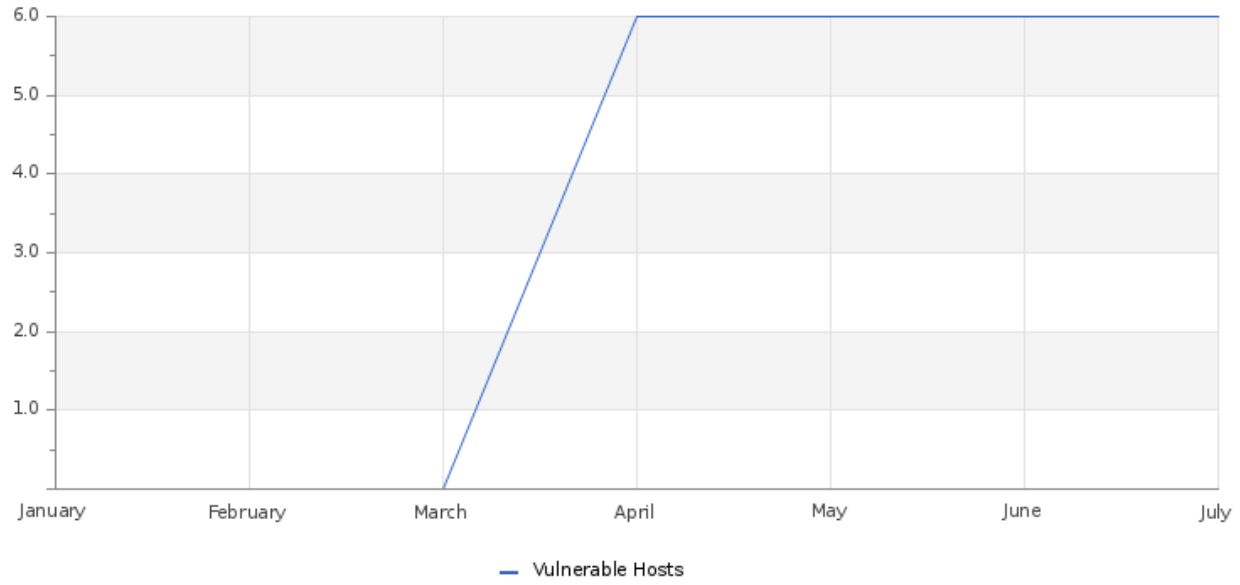
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Top 10 Most Common Vulnerabilities

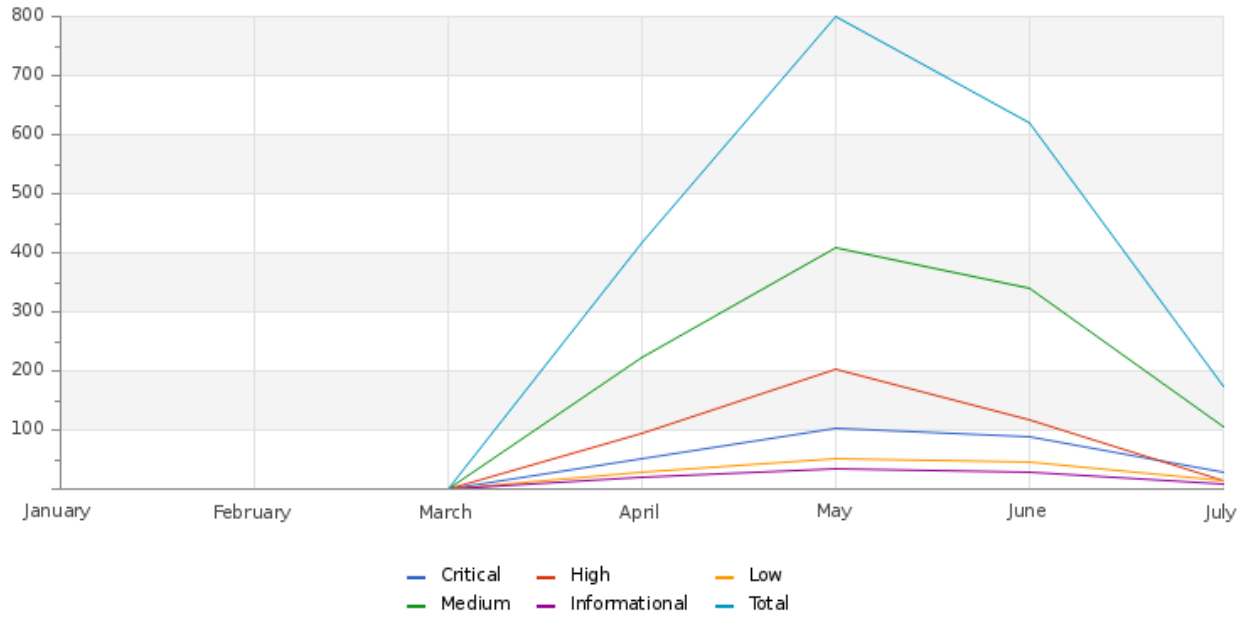
CVE	Vulnerability
CVE-2020-24113	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CVE-2023-0008	Externally Controlled Reference to a Resource in Another Sphere
CVE-2023-38046	Externally Controlled Reference to a Resource in Another Sphere
CVE-2023-48795	Improper Validation of Integrity Check Value
CVE-2023-6789	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CVE-2023-6790	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CVE-2023-6791	Insufficiently Protected Credentials
CVE-2023-6793	Improper Privilege Management
CVE-2024-0009	Improper Verification of Source of a Communication Channel
CVE-2024-3382	Allocation of Resources Without Limits or Throttling

History

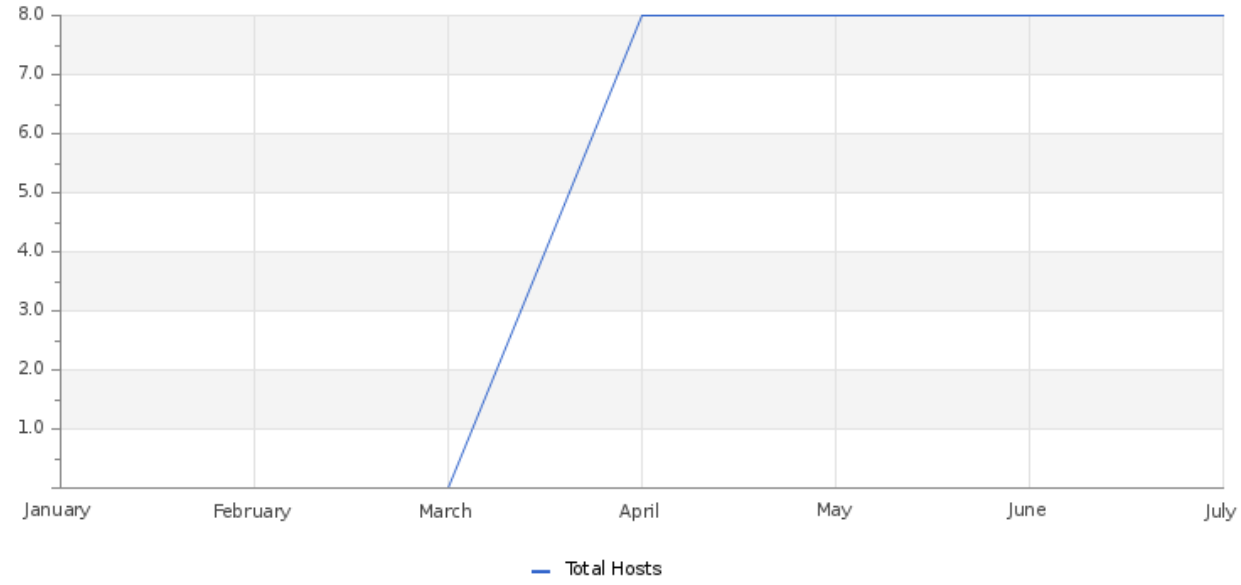
Vulnerable Host History



Vulnerable Severity History



Discovered Host History



LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

MSS-IOT REPORT

GLESEC 07/12/2024

Vulnerabilities Compared To Previous Month

dest	Previous	Current
GOC USA S&E Phone	1	1
Admin USA Phone	1	1
GOC USA Phone	1	1
GLESEC-AWS-UTM-1A	14	10
GLESEC-AWS-UTM-1B	14	10
MSS-UTM-PaloAlto-Panorama	14	10

Vulnerability Database

Vulnerability Database

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Insufficiently Protected Credentials	CVE-2023-6791	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6791	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CVE-2023-6790	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6790	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Externally Controlled Reference to a Resource in Another Sphere	CVE-2023-0008	false	https://nvd.nist.gov/vuln/detail/CVE-2023-0008	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Externally Controlled Reference to a Resource in Another Sphere	CVE-2023-38046	false	https://nvd.nist.gov/vuln/detail/CVE-2023-38046	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Critical	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Neutralization of Special Elements used in a Command ('Command Injection')	CVE-2024-3400	true	https://nvd.nist.gov/vuln/detail/CVE-2024-3400	4 day(s)	2,024/07/09 0:03:31+0000
Medium	High	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Allocation of Resources Without Limits or Throttling	CVE-2024-3382	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3382	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Verification of Source of a Communication Channel	CVE-2024-0009	false	https://nvd.nist.gov/vuln/detail/CVE-2024-0009	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Validation of Integrity Check Value	CVE-2023-48795	false	https://nvd.nist.gov/vuln/detail/CVE-2023-48795	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Low	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Privilege Management	CVE-2023-6793	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6793	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CVE-2023-6789	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6789	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Insufficiently Protected Credentials	CVE-2023-6791	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6791	4 day(s)	2,024/07/09 0:03:31+0000

TLP:AMBER

MSS-IOT REPORT

GLESEC 07/12/2024

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Medium	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CVE-2023-6790	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6790	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Externally Controlled Reference to a Resource in Another Sphere	CVE-2023-0008	false	https://nvd.nist.gov/vuln/detail/CVE-2023-0008	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Externally Controlled Reference to a Resource in Another Sphere	CVE-2023-38046	false	https://nvd.nist.gov/vuln/detail/CVE-2023-38046	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Critical	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Improper Neutralization of Special Elements used in a Command ('Command Injection')	CVE-2024-3400	true	https://nvd.nist.gov/vuln/detail/CVE-2024-3400	4 day(s)	2,024/07/09 0:03:31+0000
Medium	High	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Allocation of Resources Without Limits or Throttling	CVE-2024-3382	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3382	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Improper Verification of Source of a Communication Channel	CVE-2024-0009	false	https://nvd.nist.gov/vuln/detail/CVE-2024-0009	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Improper Validation of Integrity Check Value	CVE-2023-48795	false	https://nvd.nist.gov/vuln/detail/CVE-2023-48795	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Low	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Improper Privilege Management	CVE-2023-6793	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6793	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	192.168.10.150	Palo Alto Networks PAN-OS	MSS-UTM-PaloAlto-Panorama	Not Set	Not Set	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CVE-2023-6789	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6789	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Critical	172.28.2.92	SIP-T23G 44.84.0.125	GOC USA S&E Phone	GOC	Not Set	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CVE-2020-24113	false	https://nvd.nist.gov/vuln/detail/CVE-2020-24113	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Critical	172.28.2.124	SIP-T23G 44.84.0.125	GOC USA Phone	GOC	Not Set	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CVE-2020-24113	false	https://nvd.nist.gov/vuln/detail/CVE-2020-24113	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Insufficiently Protected Credentials	CVE-2023-6791	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6791	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CVE-2023-6790	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6790	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Externally Controlled Reference to a Resource in Another Sphere	CVE-2023-0008	false	https://nvd.nist.gov/vuln/detail/CVE-2023-0008	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Externally Controlled Reference to a Resource in Another Sphere	CVE-2023-38046	false	https://nvd.nist.gov/vuln/detail/CVE-2023-38046	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Critical	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Neutralization of Special Elements used in a Command ('Command Injection')	CVE-2024-3400	true	https://nvd.nist.gov/vuln/detail/CVE-2024-3400	4 day(s)	2,024/07/09 0:03:31+0000
Medium	High	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Allocation of Resources Without Limits or Throttling	CVE-2024-3382	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3382	4 day(s)	2,024/07/09 0:03:31+0000

MSS-IOT REPORT

GLESEC 07/12/2024

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Medium	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Verification of Source of a Communication Channel	CVE-2024-0009	false	https://nvd.nist.gov/vuln/detail/CVE-2024-0009	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Validation of Integrity Check Value	CVE-2023-48795	false	https://nvd.nist.gov/vuln/detail/CVE-2023-48795	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Low	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Privilege Management	CVE-2023-6793	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6793	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CVE-2023-6789	false	https://nvd.nist.gov/vuln/detail/CVE-2023-6789	4 day(s)	2,024/07/09 0:03:31+0000
Medium	Critical	172.28.2.89	SIP-T23G 44.84.0.125	Admin USA Phone	GOC	Not Set	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CVE-2020-24113	false	https://nvd.nist.gov/vuln/detail/CVE-2020-24113	4 day(s)	2,024/07/09 0:03:31+0000

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

GLESEC

COMPLETELY PERCEPTIVE

TLP:AMBER

MSS-IOT REPORT

HOW CAN WE HELP?

Contact us today for more information on our services and security solutions.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500