TLP:AMBER

MSS-IOT REPORT

GLESEC

March 31, 2025

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

32%

Baseline Devices

9

Vulnerable Devices

5

Executive Summary Vulnerability Severity Distribution

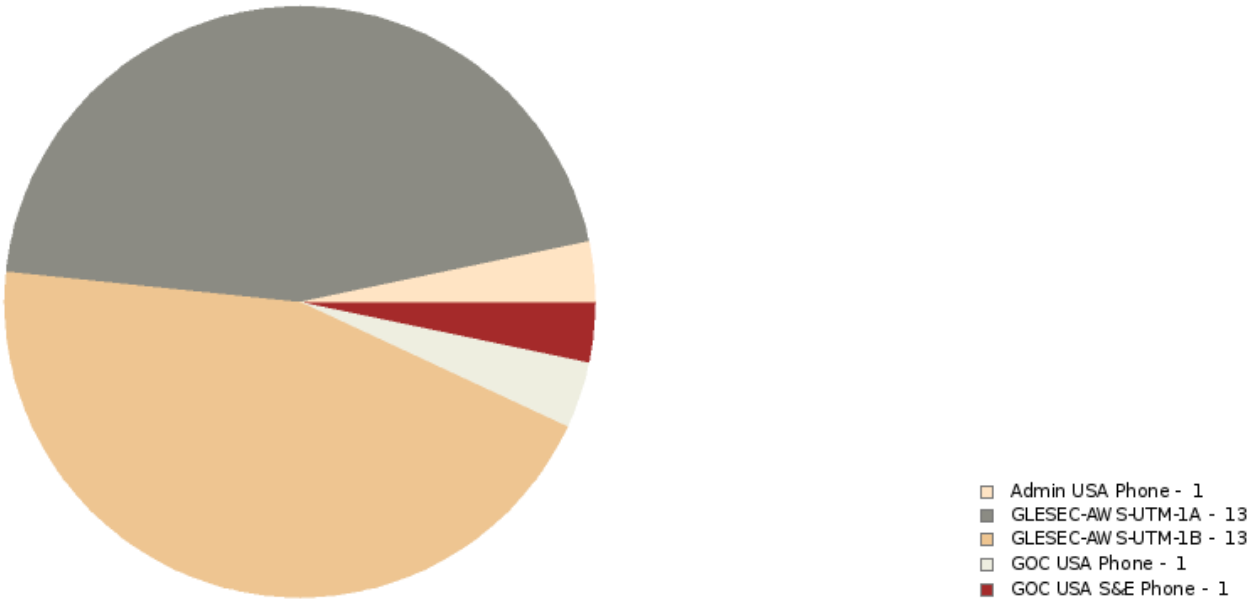
Site	critical	high	medium	low	Total
AWS	4	6	14	2	26
GOC-USA	3	0	0	0	3

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

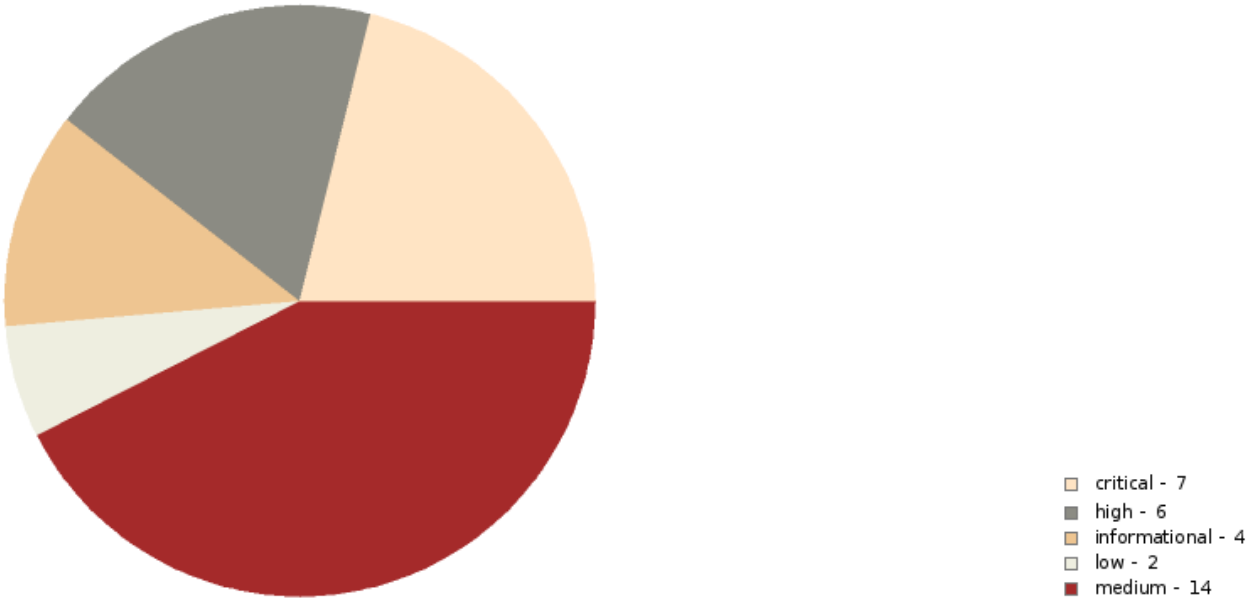
MSS-IOT REPORT

GLESEC 03/31/2025

Most Vulnerable Device *



Vulnerability Distribution



LATAM HQ
+507 836-5355

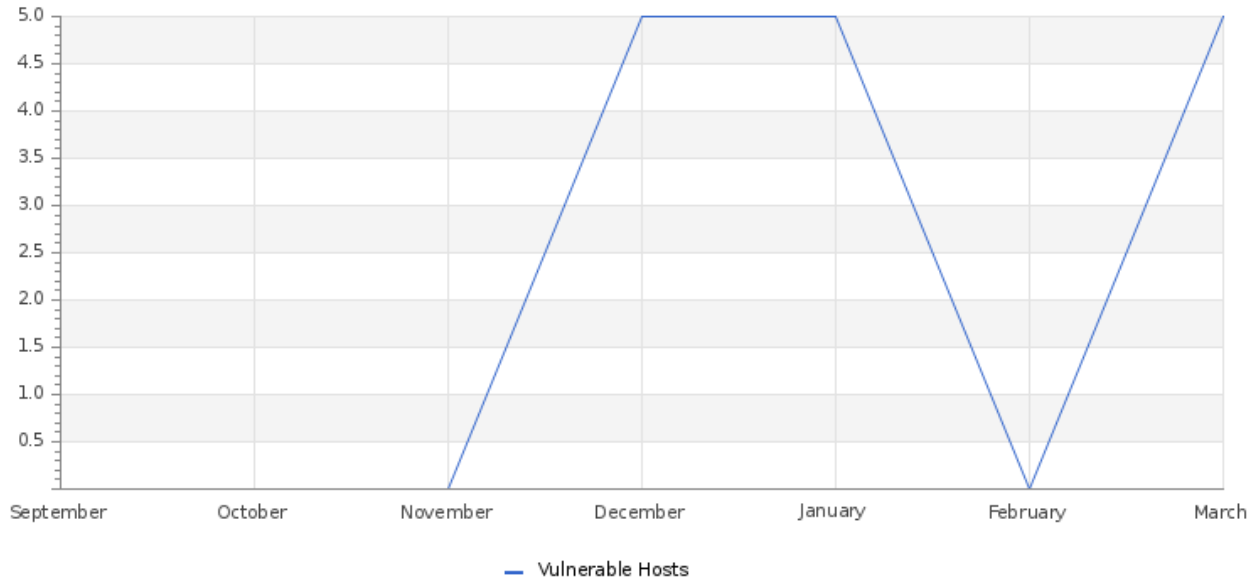
US HQ
+1 (321) 430-0500

Top 10 Most Common Vulnerabilities

CVE	Vulnerability
CVE-2020-24113	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CVE-2020-1999	Improper Check for Unusual or Exceptional Conditions
CVE-2022-0011	Interpretation Conflict
CVE-2023-6793	Improper Privilege Management
CVE-2024-0009	Origin Validation Error
CVE-2024-2550	NULL Pointer Dereference
CVE-2024-3383	Improper Ownership Management
CVE-2024-3386	Interpretation Conflict
CVE-2024-3388	Improper Privilege Management
CVE-2024-3400	Improper Neutralization of Special Elements used in a Command ('Command Injection')

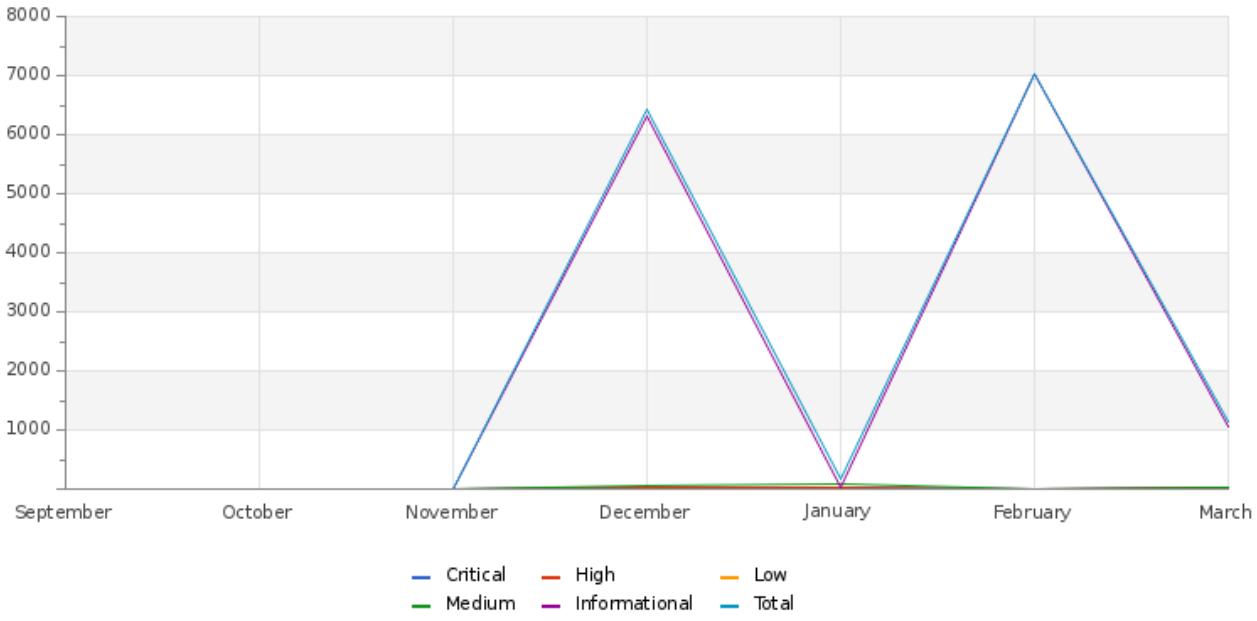
History

Vulnerable Device History

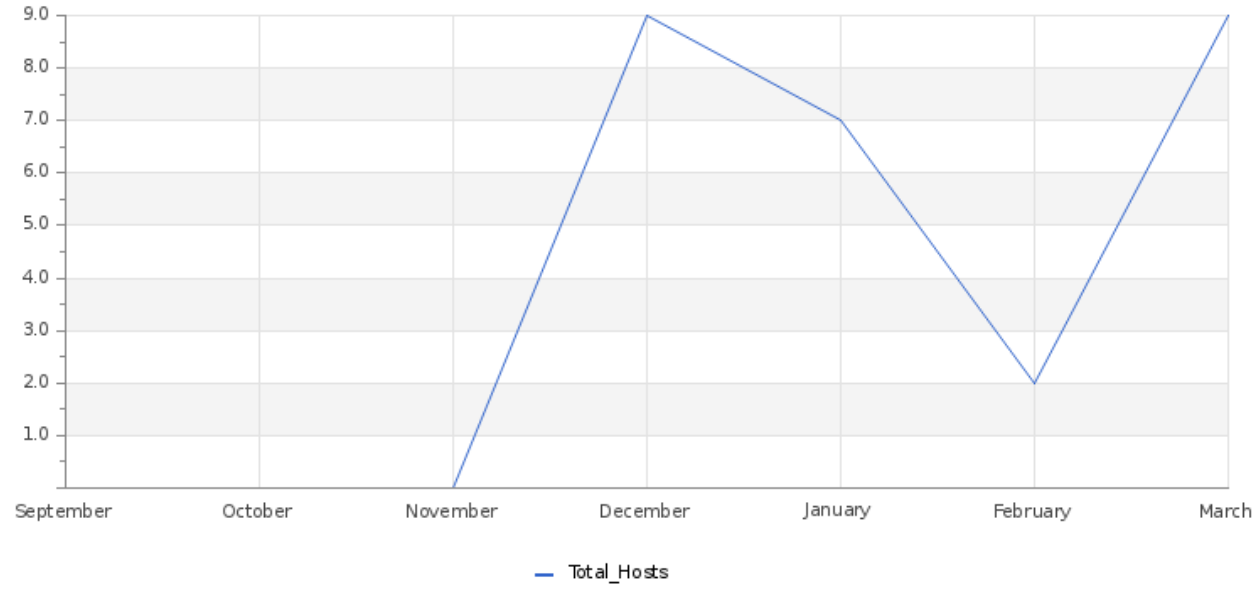


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Vulnerable Severity History



Discovered Device History



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

MSS-IOT REPORT

GLESEC 03/31/2025

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	13	13
GLESEC-AWS-UTM-1B	13	13

Vulnerability Database

Vulnerability Database

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
	Critical	172.28.2.92	SIP-T23G 44.84.0.125	GOC USA S&E Phone	Not Set	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	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	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	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Interpretation Conflict	CVE-2024-3386	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3386	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Critical	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Validation of Integrity Check Value	CVE-2024-3596	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3596	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	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	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	High	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Out-of-bounds Write	CVE-2024-9468	false	https://nvd.nist.gov/vuln/detail/CVE-2024-9468	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Origin Validation Error	CVE-2024-0009	false	https://nvd.nist.gov/vuln/detail/CVE-2024-0009	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Interpretation Conflict	CVE-2022-0011	false	https://nvd.nist.gov/vuln/detail/CVE-2022-0011	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Check for Unusual or Exceptional Conditions	CVE-2020-1999	false	https://nvd.nist.gov/vuln/detail/CVE-2020-1999	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Certificate Validation	CVE-2024-5918	false	https://nvd.nist.gov/vuln/detail/CVE-2024-5918	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	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	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Privilege Management	CVE-2024-3388	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3388	1 day(s)	2,025/03/30 0:03:20+0000

TLP:AMBER

MSS-IOT REPORT

GLESEC 03/31/2025

Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On
Not Defined	High	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Ownership Management	CVE-2024-3383	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3383	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	Improper Privilege Management	CVE-2024-9471	false	https://nvd.nist.gov/vuln/detail/CVE-2024-9471	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	High	10.100.1.234	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1A	Not Set	Not Set	NULL Pointer Dereference	CVE-2024-2550	false	https://nvd.nist.gov/vuln/detail/CVE-2024-2550	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	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	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Interpretation Conflict	CVE-2024-3386	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3386	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Critical	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Validation of Integrity Check Value	CVE-2024-3596	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3596	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	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	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	High	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Out-of-bounds Write	CVE-2024-9468	false	https://nvd.nist.gov/vuln/detail/CVE-2024-9468	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Origin Validation Error	CVE-2024-0009	false	https://nvd.nist.gov/vuln/detail/CVE-2024-0009	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Interpretation Conflict	CVE-2022-0011	false	https://nvd.nist.gov/vuln/detail/CVE-2022-0011	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Check for Unusual or Exceptional Conditions	CVE-2020-1999	false	https://nvd.nist.gov/vuln/detail/CVE-2020-1999	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Certificate Validation	CVE-2024-5918	false	https://nvd.nist.gov/vuln/detail/CVE-2024-5918	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	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	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Privilege Management	CVE-2024-3388	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3388	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	High	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Ownership Management	CVE-2024-3383	false	https://nvd.nist.gov/vuln/detail/CVE-2024-3383	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	Medium	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	Improper Privilege Management	CVE-2024-9471	false	https://nvd.nist.gov/vuln/detail/CVE-2024-9471	1 day(s)	2,025/03/30 0:03:20+0000
Not Defined	High	10.100.129.14	Palo Alto Networks PAN-OS	GLESEC-AWS-UTM-1B	Not Set	Not Set	NULL Pointer Dereference	CVE-2024-2550	false	https://nvd.nist.gov/vuln/detail/CVE-2024-2550	1 day(s)	2,025/03/30 0:03:20+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.**

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