TLP:AMBER

MSS-VME REPORT

BLADEX

June 19, 2023

TLP AMBER
MSS-VME REPORT

Sobre este reporte

Se trata de un informe SKYWATCH que presenta la información más actualizada del MSS-VME tal y como se muestra en el panel de control del servicio.

Overview

Vulnerability Level

2%

Discovered Hosts

820

Vulnerable Hosts

4

Executive Summary Vulnerability Severity Distribution

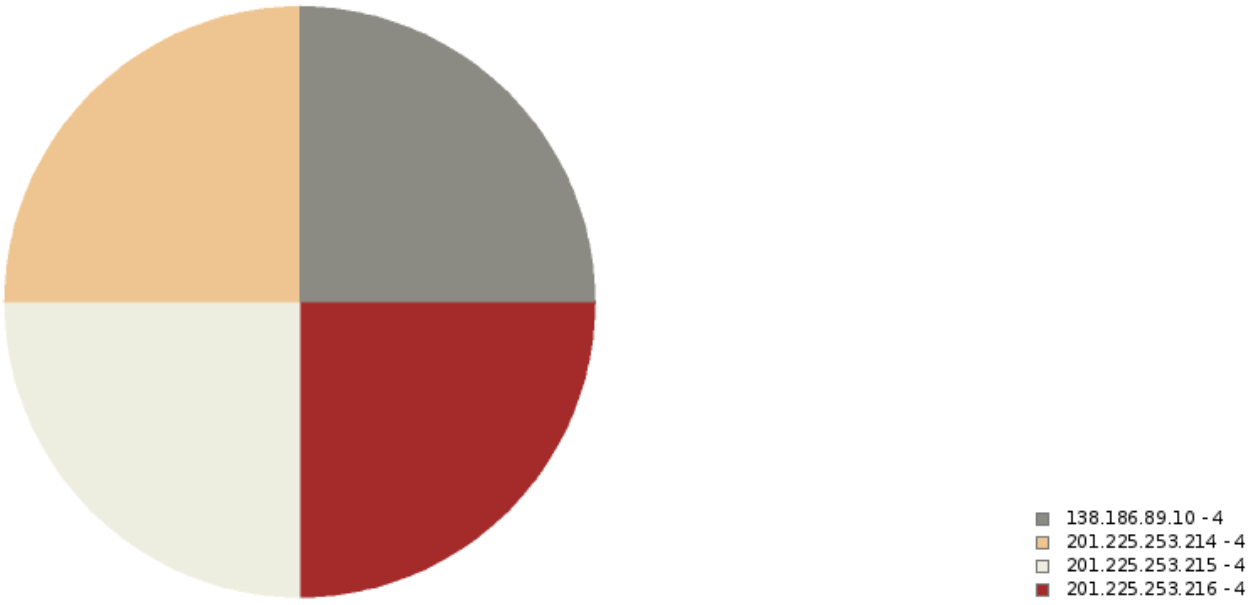
Scanner	critical	high	medium	low
BLADEX	0	0	12	4

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

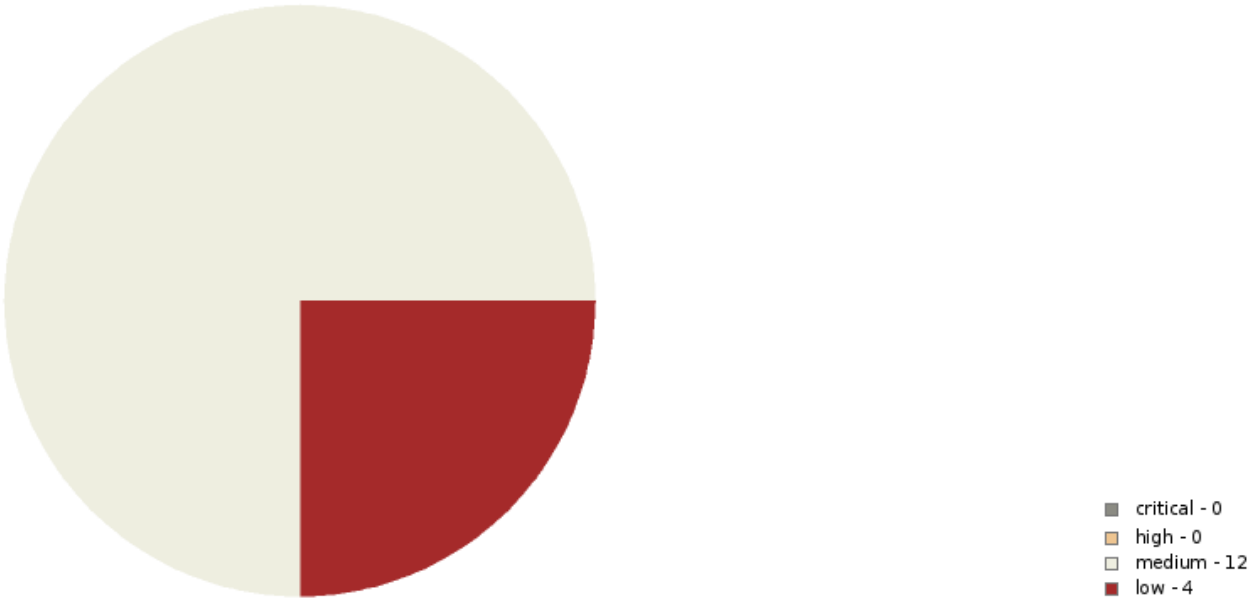
MSS-VME REPORT

BLADEX 06/19/2023

Most Vulnerable Host *



Vulnerability Distribution



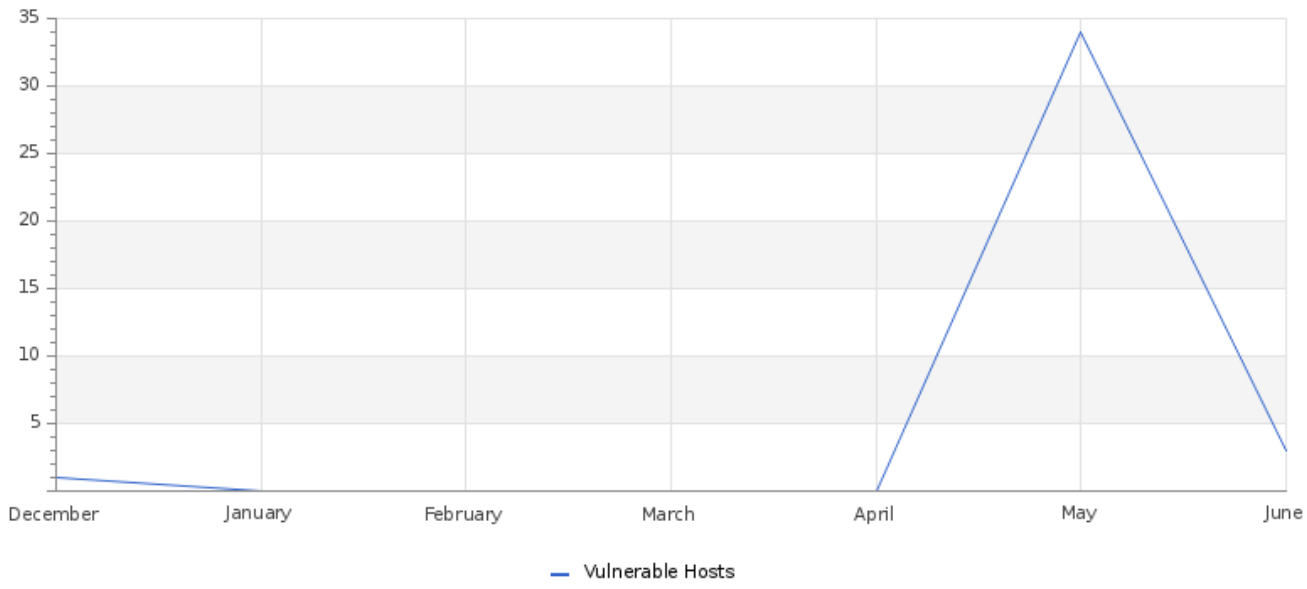
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Top 10 Most Common Vulnerabilities

Vulnerability
SSL Certificate Cannot Be Trusted
SSL Certificate Chain Contains RSA Keys Less Than 2,048 bits
SSL Certificate Signed Using Weak Hashing Algorithm
SSL Self-Signed Certificate

History

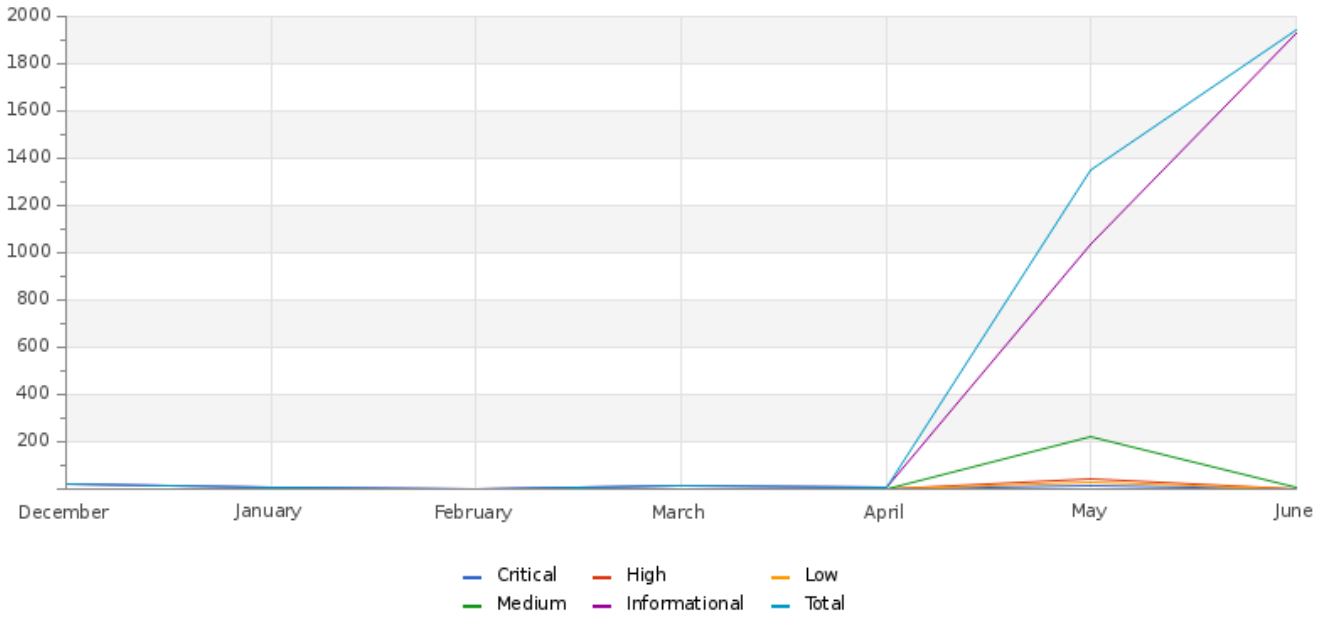
Vulnerable Host History



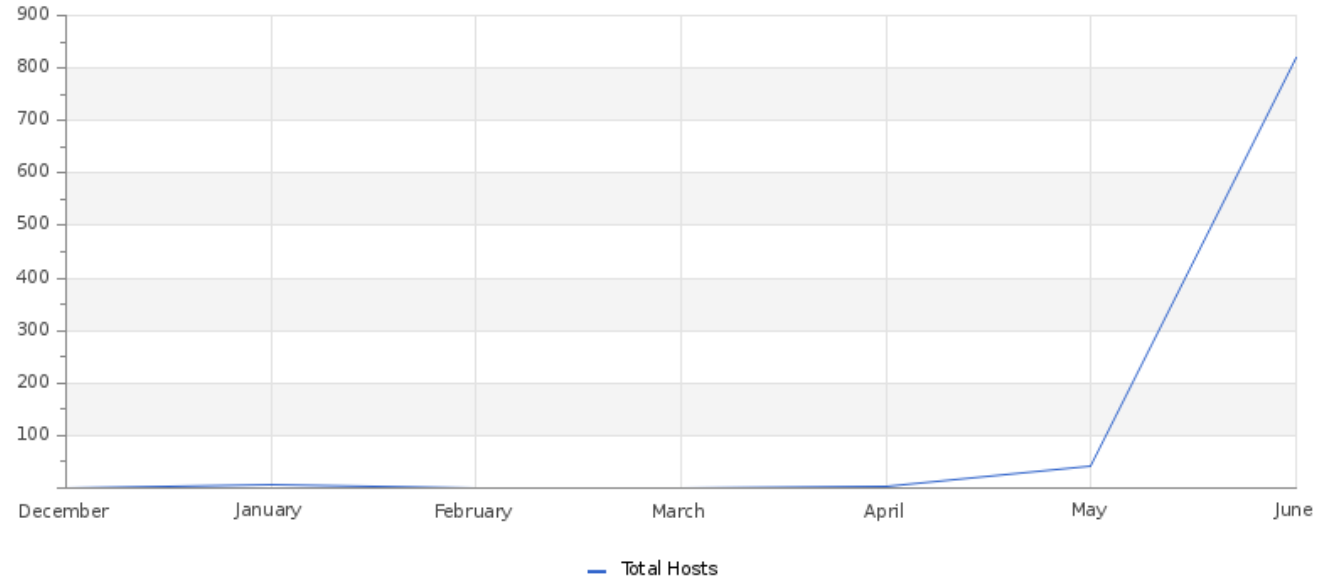
MSS-VME REPORT

BLADEX 06/19/2023

Vulnerability Severity History



Discovered Host History



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

Vulnerabilities Compared To Previous Month

dest	Previous	Current
138.186.89.10	4	4
201.225.253.214	4	4
201.225.253.215	4	4
201.225.253.216	4	4

Open Port Monitoring

Open Ports

ip	hostname	port	status	protocol	service
10.10.1.46		80	open	tcp	www
10.10.1.46		135	open	tcp	epmap
10.10.1.46		139	open	tcp	smb
10.10.1.46		445	open	tcp	cifs
10.10.1.46		1571	open	tcp	No Service Detected
10.10.1.46		2000	open	tcp	No Service Detected
10.10.1.46		2701	open	tcp	sccm_rcinfo
10.10.1.46		3389	open	tcp	No Service Detected
10.10.1.46		5985	open	tcp	www
10.10.1.46		8005	open	tcp	www
10.10.1.46		8080	open	tcp	www
10.10.1.51		22	open	tcp	ssh
10.10.1.51		80	open	tcp	www
10.10.1.51		2000	open	tcp	No Service Detected
10.10.1.53		21	open	tcp	ftp
10.10.1.53		139	open	tcp	smb
10.10.1.53		445	open	tcp	cifs
10.10.1.53		2000	open	tcp	No Service Detected
10.10.1.53		3306	open	tcp	mysql
10.10.1.53		4369	open	tcp	epmd
10.10.1.53		27017	open	tcp	mongodb
172.20.0.1		18264	open	tcp	www
10.254.0.100		18264	open	tcp	www

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

MSS-VME REPORT

BLADEX 06/19/2023

ip	hostname	port	status	protocol	service
10.220.3.10		135	open	tcp	epmap
10.51.0.121		135	open	tcp	epmap
10.51.0.75		135	open	tcp	epmap
10.10.1.27		80	open	tcp	www
10.10.1.27		135	open	tcp	epmap
10.10.1.27		139	open	tcp	smb
10.10.1.27		445	open	tcp	cifs
10.10.1.27		1801	open	tcp	msmq
10.10.1.27		2000	open	tcp	No Service Detected
10.10.1.27		2103	open	tcp	dce
10.10.1.27		2105	open	tcp	dce
10.10.1.27		2107	open	tcp	dce
10.10.1.27		2701	open	tcp	sccm_rcinfo
10.10.1.27		3389	open	tcp	No Service Detected
10.10.1.27		5985	open	tcp	www
10.10.1.27		8005	open	tcp	www
10.10.1.1		22	open	tcp	ssh
10.10.1.1		256	open	tcp	fw1_generic
10.10.1.1		257	open	tcp	fw1_generic
10.10.1.1		263	open	tcp	fw1_generic
10.10.1.1		900	open	tcp	www
10.10.1.1		2000	open	tcp	No Service Detected
10.10.1.1		18183	open	tcp	fw1_generic
10.10.1.1		18184	open	tcp	fw1_generic
10.10.1.1		18187	open	tcp	fw1_generic
10.10.1.1		18264	open	tcp	www
172.20.0.2		18264	open	tcp	www
10.254.0.101		18264	open	tcp	www
10.240.3.93		135	open	tcp	epmap
10.220.3.11		135	open	tcp	epmap
10.200.3.19		135	open	tcp	epmap
10.51.0.102		135	open	tcp	epmap

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

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

TLP:AMBER

MSS-VME 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