



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

MSS-VM REPORT

GLESEC

June 22, 2023



TLP AMBER

MSS-VM REPORT

About this report

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

Overview

Vulnerability Level

8%

Discovered Hosts

48

Vulnerable Hosts

27

EXECUTIVE SUMMARY VULNERABILITY SEVERITY DISTRIBUTION*

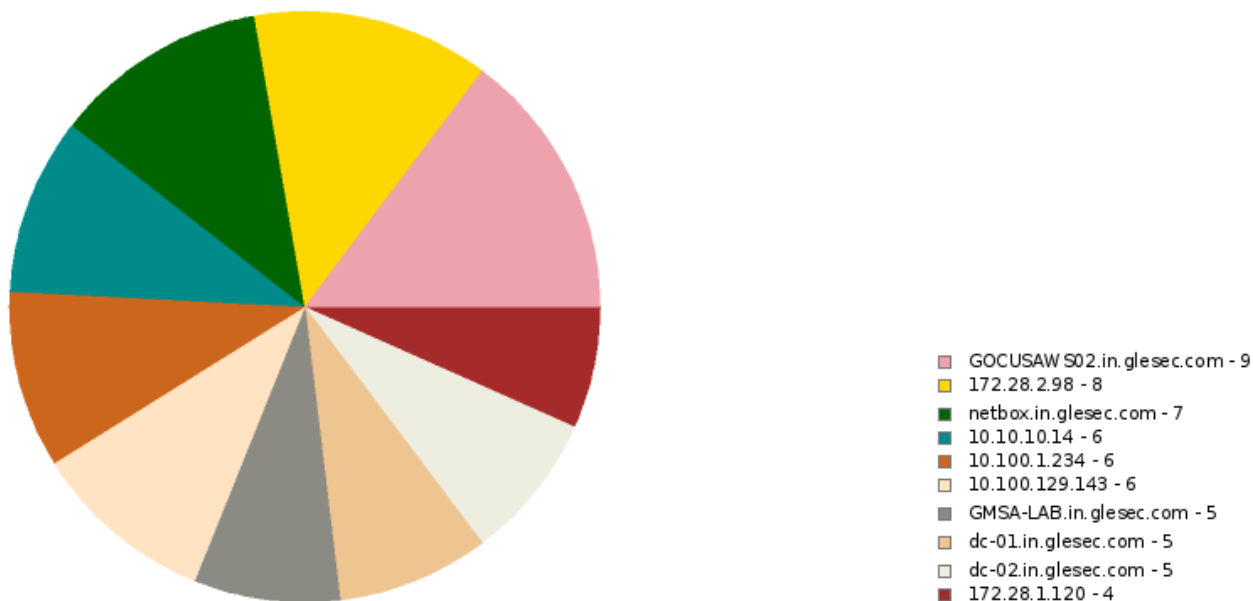
| Scanner | critical | high | medium | low | Total |
|--------------------|----------|------|--------|-----|-------|
| GLESEC | 1 | 4 | 88 | 11 | 104 |
| GLESEC WEB SERVERS | 0 | 0 | 3 | 1 | 4 |



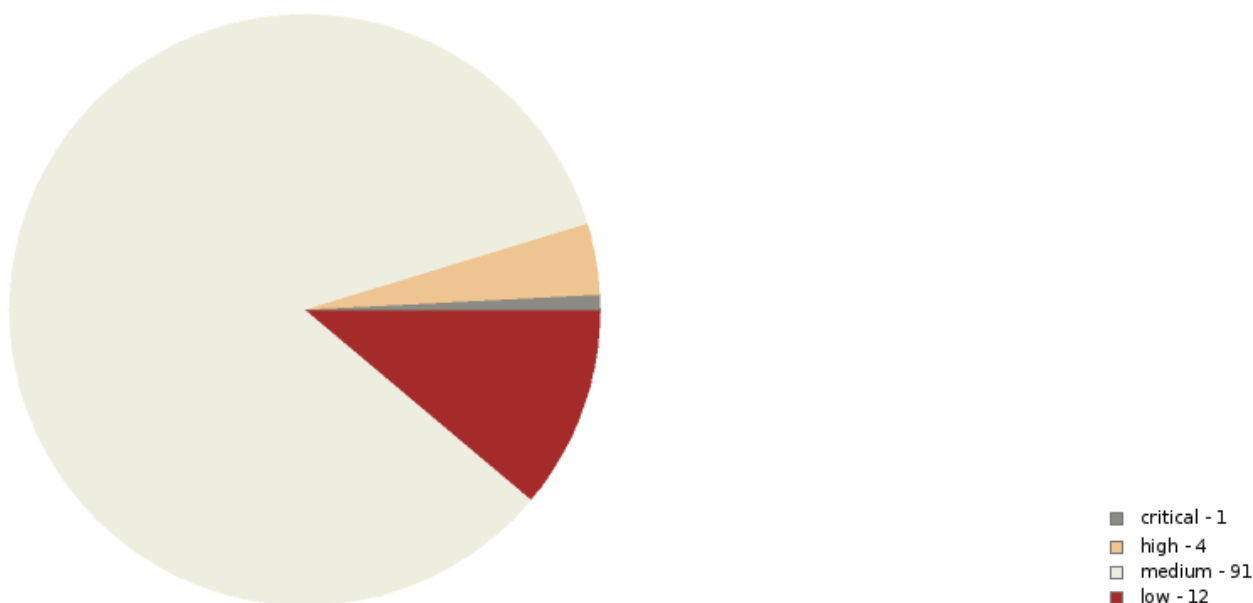
MSS-VM REPORT

GLESEC 06/22/2023

Most Vulnerable Host *



Vulnerability Distribution



MSS-VM REPORT

GLESEC 06/22/2023

Top 10 Most Common Vulnerabilities

Vulnerability

SSL Certificate Cannot Be Trusted

SSL Self-Signed Certificate

Microsoft Windows Unquoted Service Path Enumeration

Web Server Allows Password Auto-Completion

TLS Version 1.10 Protocol Deprecated

Splunk Enterprise and Universal Forwarder < 9.00 Improper Certificate Validation

Cisco AnyConnect Secure Mobility Client DoS (cisco-sa-anyconnect-dos-55AYyxYr)

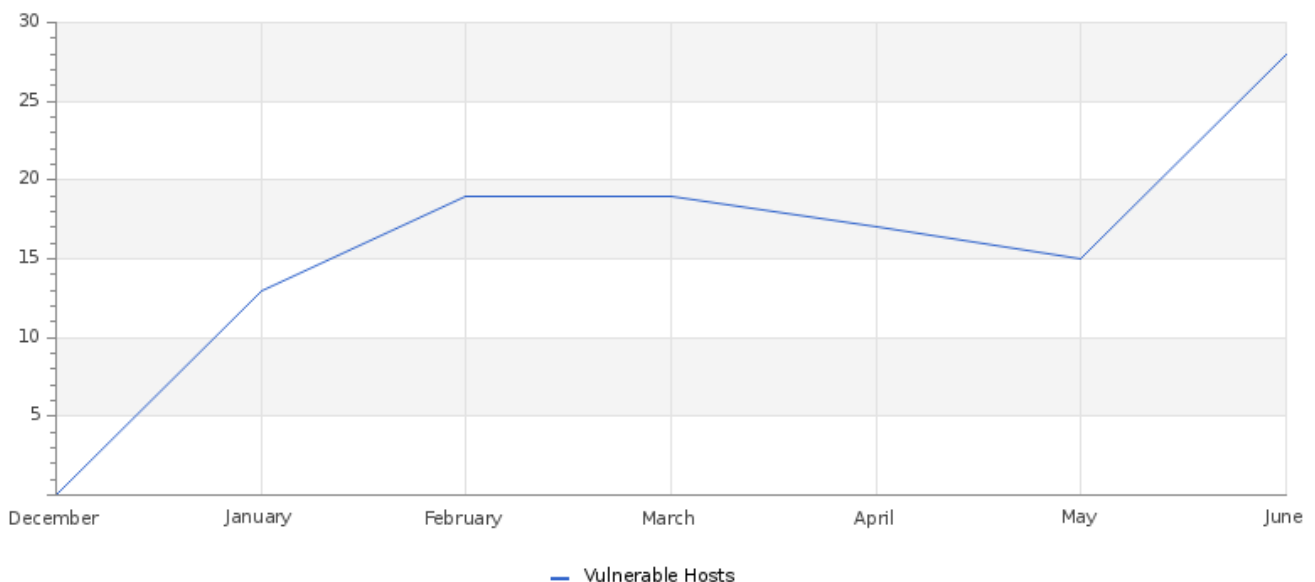
Cisco AnyConnect Secure Mobility Client Profile Modification Vulnerability (cisco-sa-anyconnect-profile-AggMUCDg)

Cisco AnyConnect Secure Mobility Client for Windows Denial of Service Vulnerability (cisco-sa-anyconnect-dos-hMHyDfb8)

Cisco AnyConnect Secure Mobility Client for Windows Privilege Escalation (cisco-sa-ac-csc-privesc-wx4U4Kw)

History

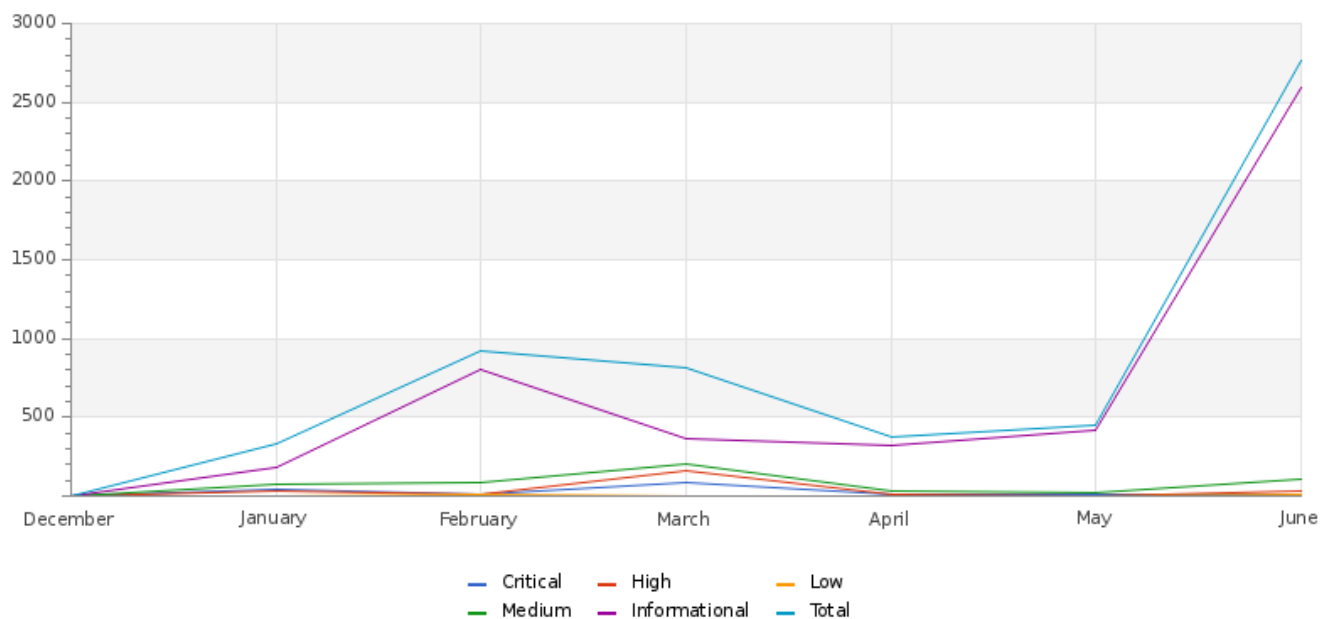
Vulnerable Host History



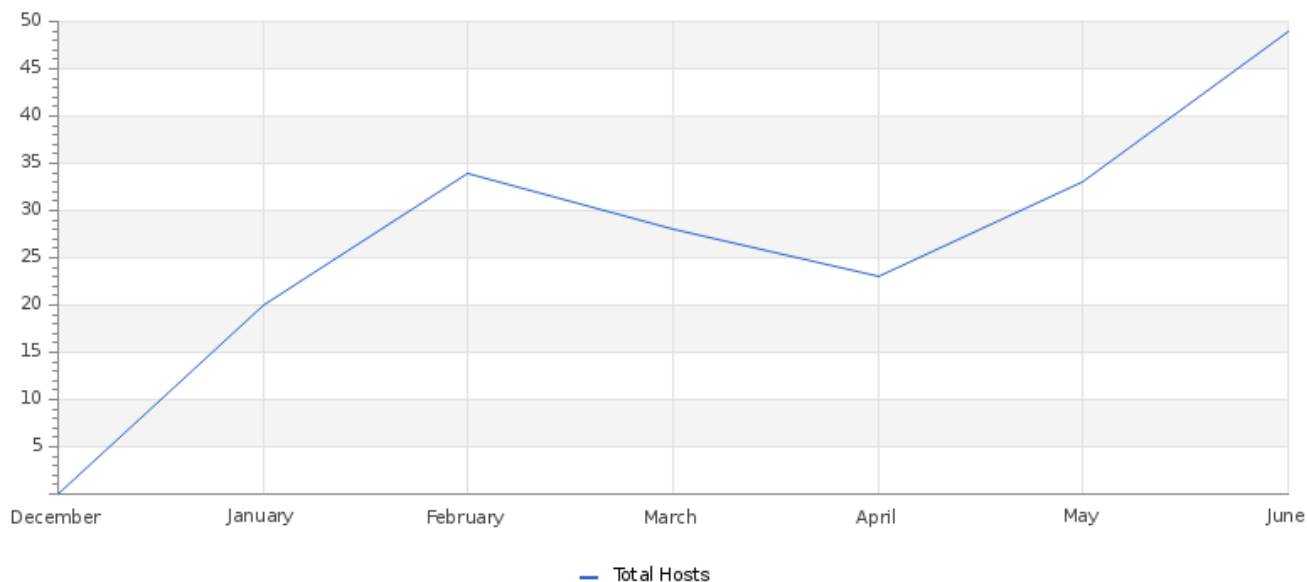
MSS-VM REPORT

GLESEC 06/22/2023

Vulnerability Severity History



Discovered Host History



MSS-VM REPORT

GLESEC 06/22/2023

Vulnerabilities Compared To Previous Month

| dest | Previous | Current |
|------------------------------|----------|---------|
| 10.10.10.14 | 6 | 6 |
| 10.100.1.185 | 2 | 2 |
| 10.100.1.234 | 6 | 6 |
| 10.100.129.14 | 2 | 2 |
| 10.100.129.143 | 6 | 6 |
| 172.28.1.119 | 7 | 3 |
| 172.28.1.120 | 2 | 4 |
| 172.28.1.65 | 1 | 1 |
| 172.28.2.124 | 2 | 2 |
| 172.28.2.65 | 2 | 3 |
| 172.28.2.92 | 2 | 2 |
| 172.28.2.98 | 9 | 8 |
| 192.168.52.28 | 7 | 4 |
| GMSA-LAB.in.glesec.com | 5 | 15 |
| GOCUSAWS02.in.glesec.com | 10 | 9 |
| PRTG.in.glesec.com | 4 | 4 |
| USASYSTEMSWS01.in.glesec.com | 6 | 4 |
| USASYSTEMSWS02.in.glesec.com | 5 | 4 |
| USASYSTEMSWS03.in.glesec.com | 6 | 4 |
| dc-01.in.glesec.com | 5 | 5 |
| dc-02.in.glesec.com | 4 | 5 |
| gmp.glesec.com | 1 | 0 |
| goc-usa-sw.in.glesec.com | 2 | 2 |
| netbox.in.glesec.com | 4 | 7 |

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.**





GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

MSS-VM REPORT

HOW CAN WE HELP?

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

