GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

ASSET REPORT 66.22.79.162

GLESEC

November 22, 2024

ASSET REPORT 66.22.79.162

GLESEC 11/22/2024

Device Profile

IP Address of System:	66.22.79.162	(Domain) Name of System:	skywatch.glesec.com
Open Ports Authorized:		Open Ports:	80, 443
Mac Address:		Operating System:	Linux Kernel 2.6
Impact:	Critical	Date Scanned:	2024-11-20 00:00:00
Location:	External	Division:	S&E
Type of System:	IT	Vendor:	
Model:		Version:	
Description of use or application of the system:			

System Vulnerabilities

Case Date Opened	Vulnerability	Case	Priority	Status
2023-09-25 00:22:01		#9673	High	Closed
2024-03-04 00:05:59		#13321	Medium	Closed

Risk

Severity	Weight
Low	**17.65**

Vulnerabilities

CVE	Severity	Criticality	Name
	medium	null	HSTS Missing From HTTPS Server (RFC 6797)
CVE-1999-0524	low	null	ICMP Timestamp Request Remote Date Disclosure
	informational	null	Service Detection
	informational	null	Common Platform Enumeration (CPE)
	informational	null	Device Type
	informational	null	HSTS Missing From HTTPS Server
	informational	null	HTTP Cookie 'secure' Property Transport Mismatch
	informational	null	HTTP Methods Allowed (per directory)
	informational	null	HTTP Server Type and Version
	informational	null	HyperText Transfer Protocol (HTTP) Information
	informational	null	Nessus Scan Information
	informational	null	Nessus SYN scanner
	informational	null	OS Identification
	informational	null	SSL / TLS Versions Supported
	informational	null	SSL Certificate Information
	informational	null	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
	informational	null	SSL Cipher Suites Supported
	informational	null	SSL Perfect Forward Secrecy Cipher Suites Supported
	informational	null	SSL Root Certification Authority Certificate Information
	informational	null	SSL/TLS Recommended Cipher Suites
	informational	null	Strict Transport Security (STS) Detection
	informational	null	TCP/IP Timestamps Supported
	informational	null	TLS ALPN Supported Protocol Enumeration
	informational	null	TLS Version 1.2 Protocol Detection
	informational	null	TLS Version 1.3 Protocol Detection
	informational	null	Traceroute Information
	informational	null	Web Application Cookies Not Marked Secure
	informational	null	Web Server Crafted Request Vendor/Version Information Disclosure
	informational	null	Web Server Directory Enumeration
	informational	null	Web Server No 404 Error Code Check

Threats

Service	Type	Severity
MSS-BOT	Spoofed browser/User Agent	medium
MSS-WAF-Cloud	Access Control	high
MSS-BOT	Known Anomalous User Agents	medium
MSS-WAF-Cloud	Misconfiguration	high
MSS-BOT	Programmatic slow bots with signature tampering	medium
MSS-WAF-Cloud	Logical Attacks	high
MSS-WAF-Cloud	HTTP RFC Violations	low
MSS-BOT	Anomalous user behavior	high
MSS-WAF-Cloud	XML & Web Services	high
MSS-WAF-Cloud	Session Management	high
MSS-BOT	Fingerprint test failed / Dynamic Turing test failed	medium
MSS-WAF-Cloud	Path Traversal	high
MSS-WAF-Cloud	Evasion	high
MSS-WAF-Cloud	Authentication & Authorization	high
MSS-WAF-Cloud	HTTP RFC Violations	high
MSS-WAF-Cloud	Unvalidated Redirect	medium
MSS-BOT	Fingerprint test failed / Dynamic Turing test failed, Spoofed browser/User Agent	medium
MSS-WAF-Cloud	Injections	high
MSS-WAF-Cloud	Cross Site Scripting	high
MSS-WAF-Cloud	DoS	high
MSS-WAF-Cloud	Information Leakage	high
MSS-WAF-Cloud	Input Validation	high
MSS-WAF-Cloud	Unvalidated Redirect	high
MSS-BOT	JavaScript Parameter Anomaly	high
MSS-BOT	Fingerprint test failed / Dynamic Turing test failed	high
MSS-BOT	Outdated Browser Versions	medium
MSS-BOT	Rate-limiting, User Session Cookie Rate limiting	high
MSS-BOT	Static User Session Cookie from multiple User Agent sources	high
MSS-DDOS-Cloud	Anomalies	medium
MSS-WAF-Cloud	File Upload Violation	high
MSS-WAF-Cloud	Intrusions	high

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

ASSET REPORT 66.22.79.162

HOW CAN WE HELP?

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