Date of Report: April 3, 2026

Contact Person

Full name
Ahmed Emad Nasr

Job title / role
Incident Response Analyst

Department / team
Security Operations Center (SOC)

Email address
Ahmed.em.nasr@gmail.com

Phone number
+201018166445

The Incident

Date and time discovered:
Mar, 07, 2024, 12:51 PM.

How was the incident detected? (E.g., user report, monitoring system alert)

A high-level security alert was triggered in the Monitoring system under the rule "SOC127 - SQL Injection Detected".

Detailed description of the incident (include what occurred, where, and how):

- An external source IP (118.194.247.28) sent a malicious HTTP GET request targeting the internal destination address 172.16.20.12 (Hostname: WebServer1000).
- The request URL contained a heavily encoded payload attempting multiple web attacks simultaneously, including SQL Injection (UNION ALL SELECT, information_schema.tables), Cross-Site Scripting (<script>alert("XSS")</script>), and Command Execution (xp_cmdshell attempting to read /etc/passwd).
- The Device Action for this request was logged as "Allowed", and the web server returned an HTTP 200 response.
- The source IP (118.194.247.28) originates from China (AS 4808) and is flagged as malicious by 9 out of 94 security vendors on VirusTotal.

Was the incident ongoing at the time of report?

☐ Yes ☒ No

Have any files, accounts, or systems been compromised?

☒ Yes ☐ No

If yes, please describe:

-
  - The malicious request was "Allowed" through the security controls.
  - *Note:* While the terminal history for 172.16.20.12 (Atlanta-Server) shows older baseline activity from 2023-11-10, the HTTP 200 response to the malicious payload on Mar 07, 2024, necessitates treating the server as potentially compromised pending deeper forensic review.

Notification

Notification

Was your supervisor or manager notified?

☒ Yes ☐ No

Date/time of notification:
April 3, 2026

Was the IT/security team alerted?

☒ Yes ☐ No

If yes, who was contacted and how? (e.g., email, phone, ticket)
Escalated to the Incident Response team via Case Management for immediate containment.

Containment Measures

What immediate actions were taken to contain the threat? (E.g., system shutdown, network isolation)

- Isolate WebServer1000 (172.16.20.12) from the network to prevent potential lateral movement or data exfiltration.
- Block the malicious source IP (118.194.247.28) on the perimeter firewall and Web Application Firewall (WAF).

Were any user accounts disabled, firewalls updated, or services suspended?

☒ Yes ☐ No

If yes, provide details:

- Firewall and WAF rules updated to drop traffic from the attacking IP.
- Vulnerability assessment required on the web application to patch the injection flaw.

Impacted Services Measures

List any systems, devices, or applications affected by the incident:

-

WebServer1000 / Atlanta-Server (IP: 172.16.20.12).

Estimated number of affected users, if applicable:

Unknown (Depends on what data the web application processes).

Was there any known data loss or exposure?

☐ Yes ☒ No

If yes, describe the type of data (e.g., personal info, credentials, financial):

The payload specifically targeted database schemas (information_schema.tables) and system configuration files (/etc/passwd), indicating an intent to expose sensitive system data.

Preliminary Analysis *(Optional)*

Suspected cause or entry point (e.g., phishing email, unpatched software):

-

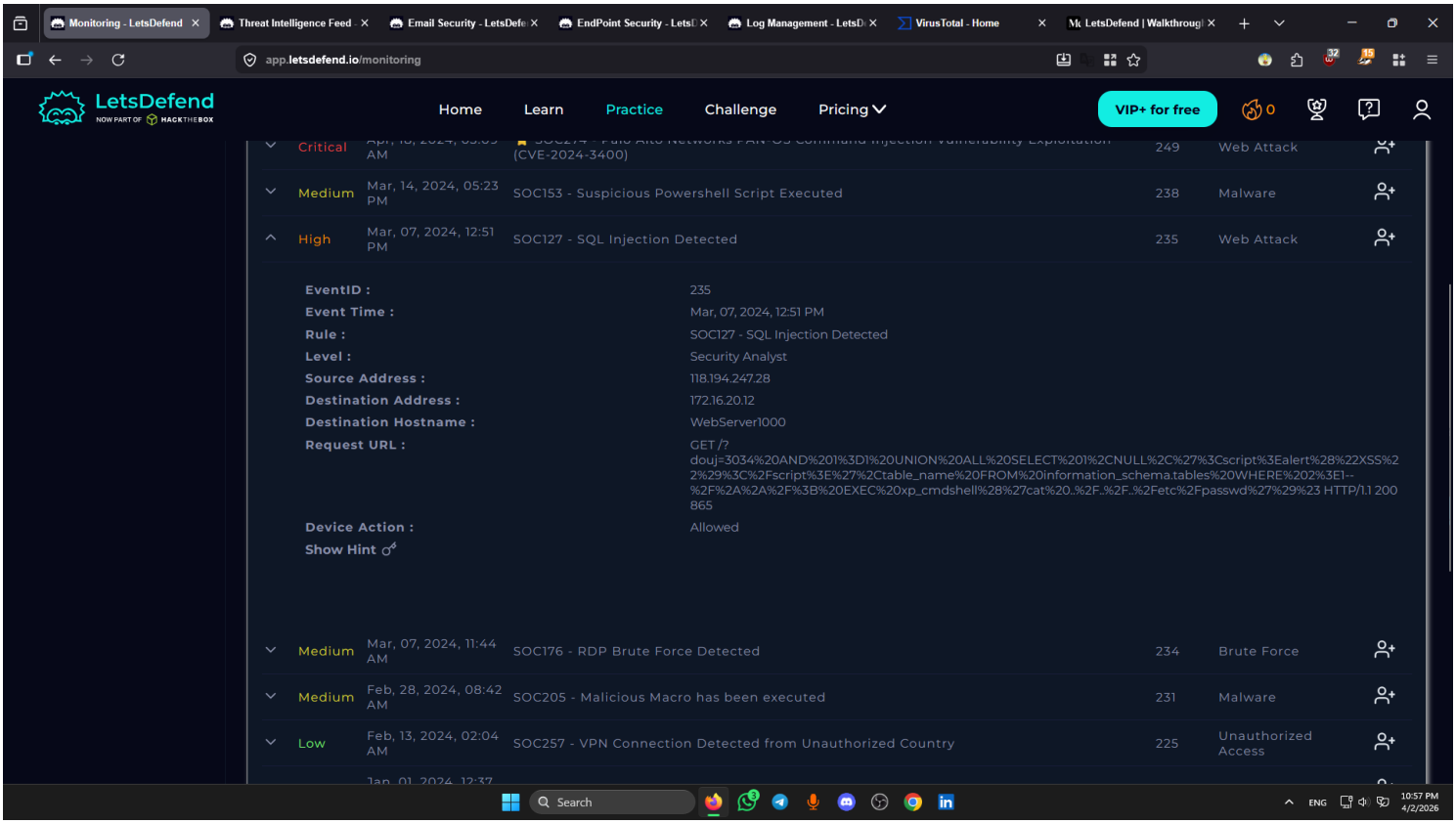
Unpatched input validation vulnerability in the web application hosted on WebServer1000, allowing for SQL Injection and Command Execution via HTTP GET parameters.

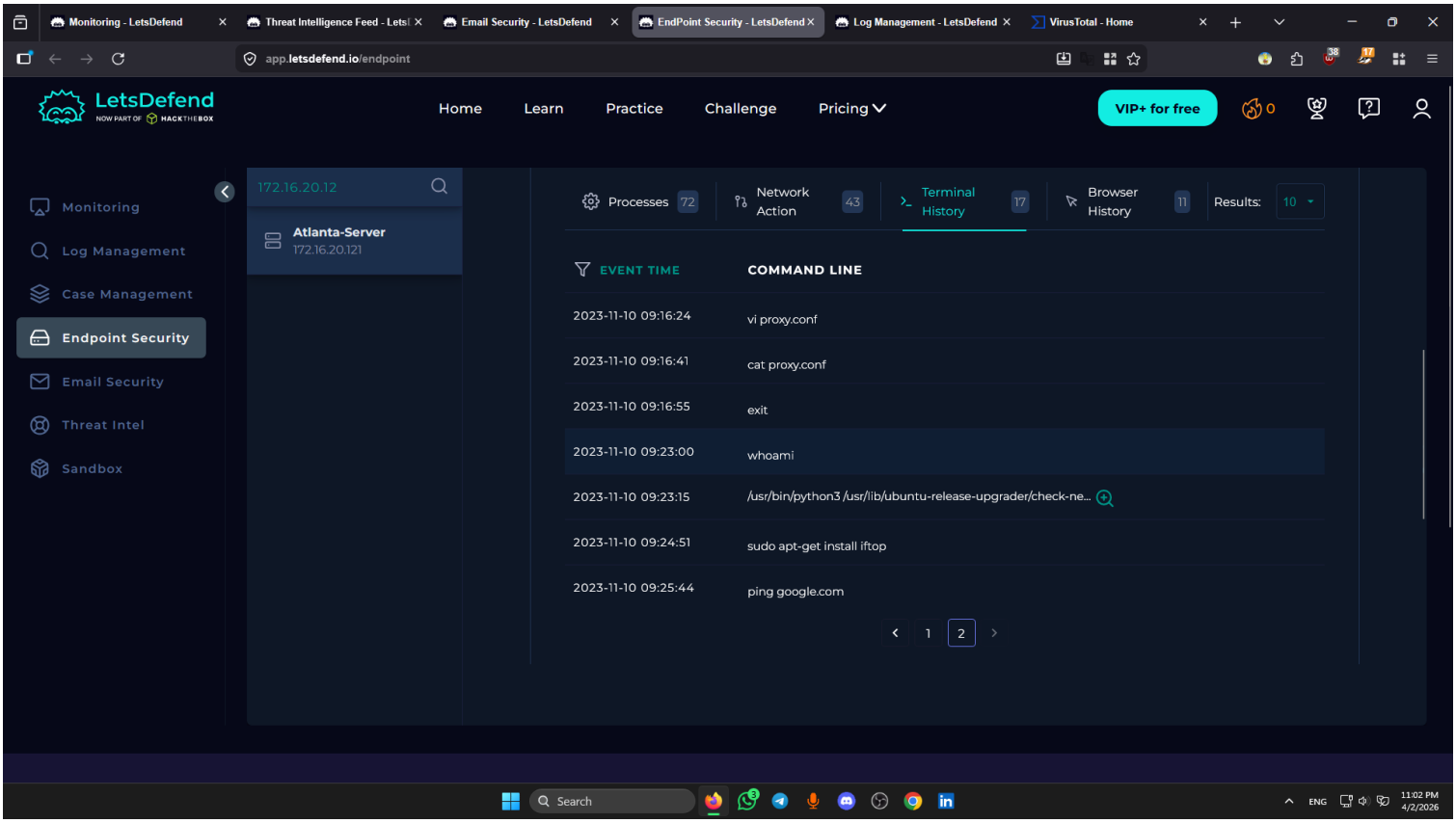
Was the threat internal, external, or unknown?

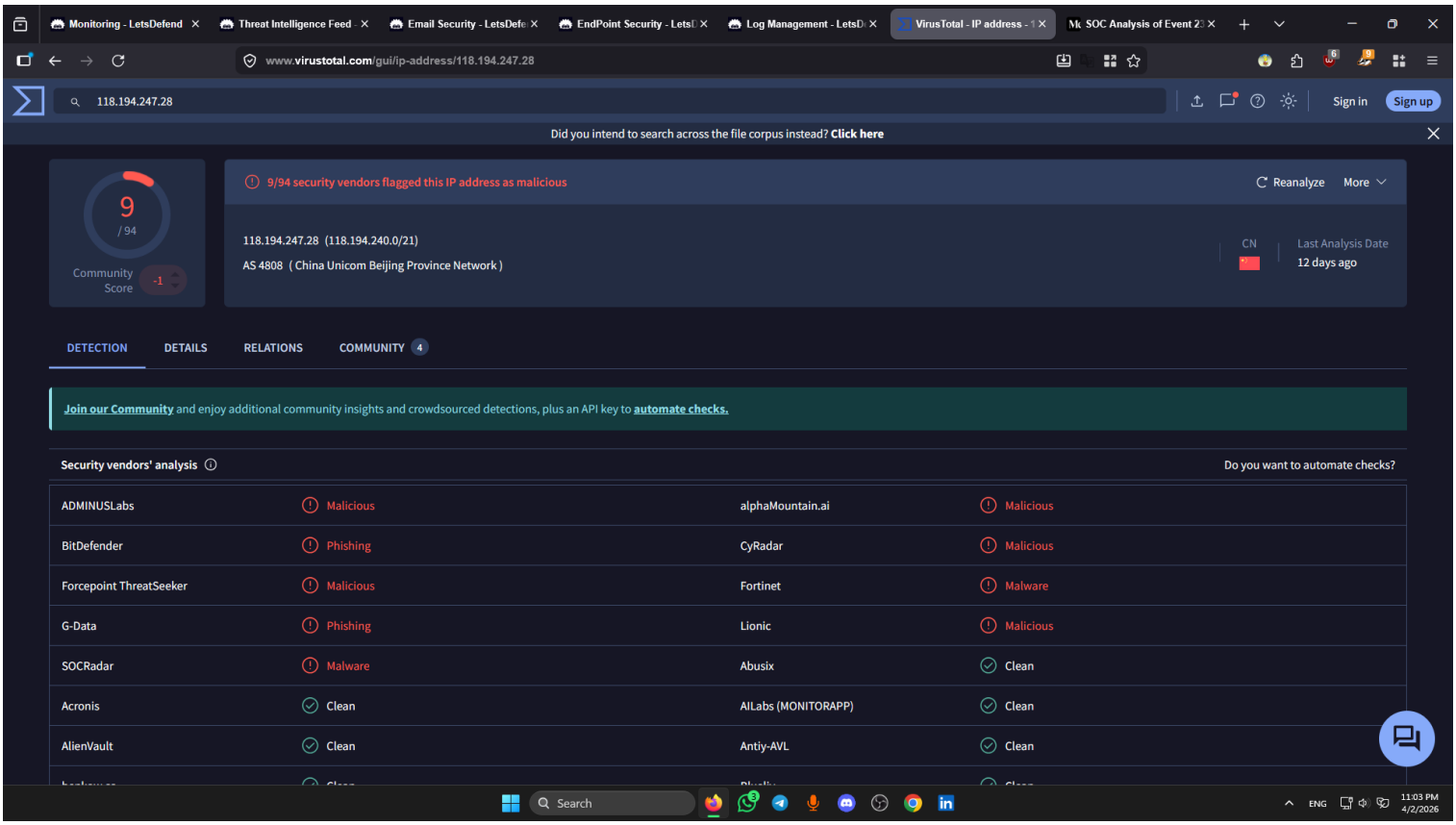
☐ Internal ☒ External ☐ Unknown

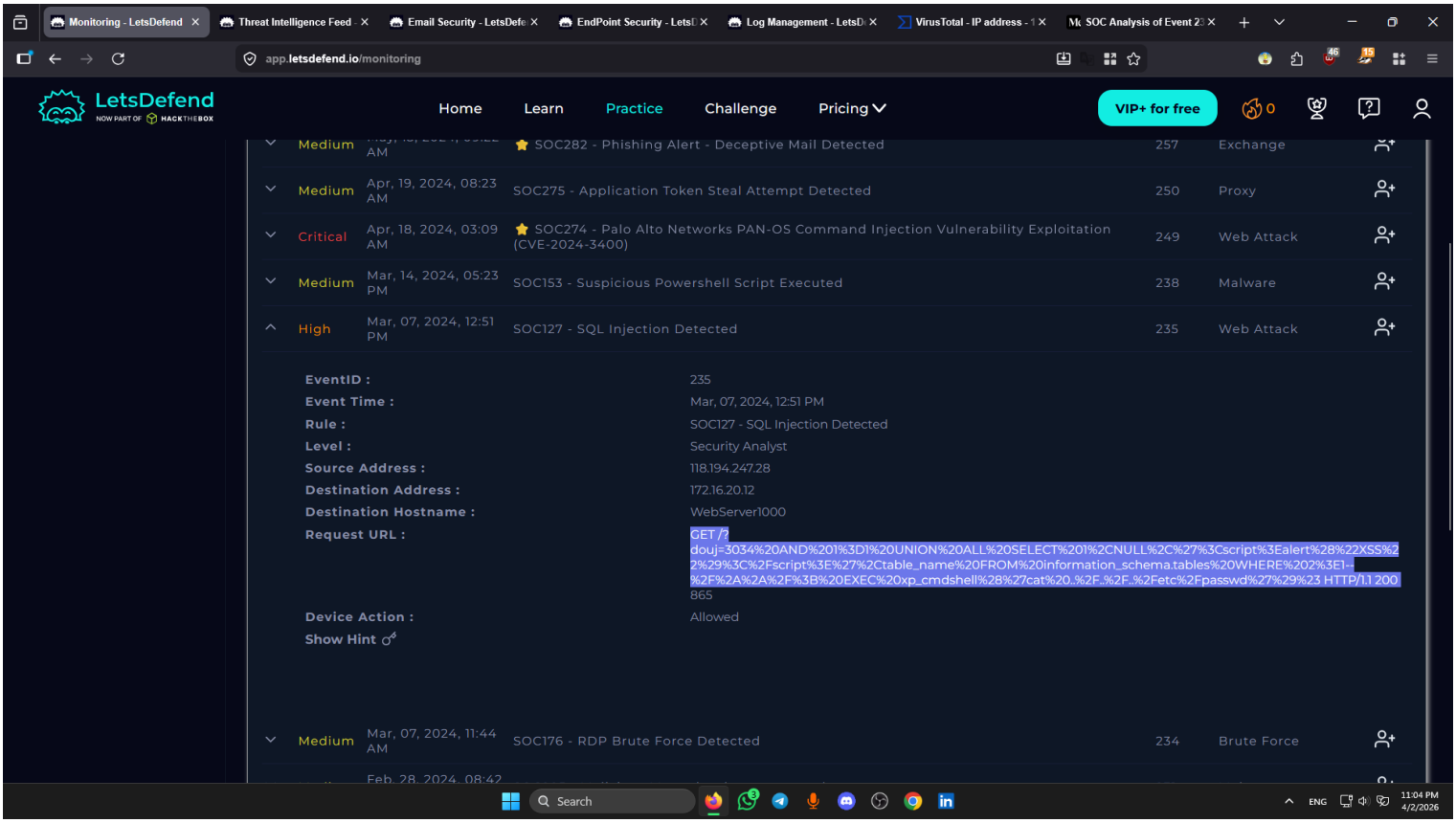
Submitted by:

Ahmed Emad Nasr	Ahmed Emad Nasr	April 3, 2026
Name	**Signature**	**Date submitted**


Monitoring - LetsDefend
Threat Intelligence Feed
Email Security - LetsDefe
EndPoint Security - LetsD
Log Management - LetsD
VirusTotal - Home
LetsDefend | Walkthrough
app.letsdefend.io/monitoring
LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Critical AM (CVE-2024-3400) 249 Web Attack
Medium Mar, 14, 2024, 05:23 PM SOC153 - Suspicious Powershell Script Executed 238 Malware
High Mar, 07, 2024, 12:51 PM SOC127 - SQL Injection Detected 235 Web Attack
EventID : 235
Event Time : Mar, 07, 2024, 12:51 PM
Rule : SOC127 - SQL Injection Detected
Level : Security Analyst
Source Address : 118.194.247.28
Destination Address : 172.16.20.12
Destination Hostname : WebServer1000
Request URL : GET /?douj=3034%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 HTTP/1.1 200 865
Device Action : Allowed
Show Hint
Medium Mar, 07, 2024, 11:44 AM SOC176 - RDP Brute Force Detected 234 Brute Force
Medium Feb, 28, 2024, 08:42 AM SOC205 - Malicious Macro has been executed 231 Malware
Low Feb, 13, 2024, 02:04 AM SOC257 - VPN Connection Detected from Unauthorized Country 225 Unauthorized Access
Search
ENG
10:57 PM
4/2/2026


Monitoring - LetsDefend
Threat Intelligence Feed - Lets
Email Security - LetsDefend
EndPoint Security - LetsDefend
Log Management - LetsDefend
VirusTotal - Home
app.letsdefend.io/endpoint
LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
172.16.20.12
Atlanta-Server
172.16.20.121
Processes 72
Network Action 43
Terminal History 17
Browser History 11
Results: 10
EVENT TIME
COMMAND LINE
2023-11-10 09:16:24 vi proxy.conf
2023-11-10 09:16:41 cat proxy.conf
2023-11-10 09:16:55 exit
2023-11-10 09:23:00 whoami
2023-11-10 09:23:15 /usr/bin/python3 /usr/lib/ubuntu-release-upgrader/check-ne...
2023-11-10 09:24:51 sudo apt-get install iftop
2023-11-10 09:25:44 ping google.com
1
2
Search
ENG
11:02 PM
4/2/2026


Monitoring - LetsDefend
Threat Intelligence Feed
Email Security - LetsDefe
EndPoint Security - LetsD
Log Management - LetsD
VirusTotal - IP address - 1
SOC Analysis of Event 2
www.virustotal.com/gui/ip-address/118.194.247.28
118.194.247.28
Sign in
Sign up
Did you intend to search across the file corpus instead? Click here
9
/ 94
Community Score
-1
9/94 security vendors flagged this IP address as malicious
Reanalyze
More
118.194.247.28 (118.194.240.0/21)
AS 4808 (China Unicom Beijing Province Network)
CN
Last Analysis Date
12 days ago
DETECTION
DETAILS
RELATIONS
COMMUNITY 4
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
ADMINUSLabs Malicious
alphaMountain.ai Malicious
BitDefender Phishing
CyRadar Malicious
Forcepoint ThreatSeeker Malicious
Fortinet Malware
G-Data Phishing
Lionic Malicious
SOCRadar Malware
Abusix Clean
Acronis Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
Antiy-AVL Clean
Search
ENG
11:03 PM
4/2/2026


Monitoring - LetsDefend
Threat Intelligence Feed
Email Security - LetsDefe
EndPoint Security - LetsD
Log Management - LetsD
VirusTotal - IP address - 1
SOC Analysis of Event 2
app.letsdefend.io/monitoring
LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Medium SOC282 - Phishing Alert - Deceptive Mail Detected 257 Exchange
Medium Apr, 19, 2024, 08:23 AM SOC275 - Application Token Steal Attempt Detected 250 Proxy
Critical Apr, 18, 2024, 03:09 AM SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400) 249 Web Attack
Medium Mar, 14, 2024, 05:23 PM SOC153 - Suspicious Powershell Script Executed 238 Malware
High Mar, 07, 2024, 12:51 PM SOC127 - SQL Injection Detected 235 Web Attack
EventID : 235
Event Time : Mar, 07, 2024, 12:51 PM
Rule : SOC127 - SQL Injection Detected
Level : Security Analyst
Source Address : 118.194.247.28
Destination Address : 172.16.20.12
Destination Hostname : WebServer1000
Request URL : GET /?douj=3034%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 HTTP/1.1 200 865
Device Action : Allowed
Show Hint
Medium Mar, 07, 2024, 11:44 AM SOC176 - RDP Brute Force Detected 234 Brute Force
Search
ENG
11:04 PM
4/2/2026