SECURITY INCIDENT REPORT

Incident ID:	INC-000110
Severity:	HIGH
Status:	OPEN
Detection Time:	2026-02-01 14:44:10 UTC
Endpoint:	EP-0027
Attack Type:	privilege_escalation

Report Generated: 2026-02-01 14:44:48

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0027** at 2026-02-01 14:44:10 UTC. The anomaly detection system identified suspicious behavior with an ensemble confidence of **93.2%**.

The system detected **3** MITRE ATT&CK; technique(s) associated with this incident, with the primary technique being **Resource Hijacking**.

Current Status: **OPEN**
Severity Classification: **HIGH**

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	0.952
Isolation Forest	0.672
LOF	0.729
Ensemble	**0.784**
Confidence	**93.2%**

MITRE ATT&CK; TECHNIQUES

T1496: Resource Hijacking

Tactic: Impact
Confidence: 88.1%
Matched Features: process_creation, memory_usage
Description: Adversaries may leverage the resources of co-opted systems to solve resource intensive problems, which may impact system availability.

T1021: Remote Services

Tactic: Lateral Movement
Confidence: 85.5%
Matched Features: process_creation, failed_logins
Description: Adversaries may use valid accounts to log into a service specifically designed to accept remote connections.

T1110: Brute Force

Tactic: Credential Access
Confidence: 62.7%

Matched Features: network_in
Description: Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Process Creation	25.50	5.00	5.10x	21.6%
Failed Logins	1.35	0.50	2.69x	13.5%
Network In	354.80	150.00	2.37x	11.8%
Api Calls	227.46	100.00	2.27x	11.4%
Memory Usage	100.00	45.00	2.22x	11.1%
Auth Attempts	4.38	2.00	2.19x	10.9%
File Access	81.61	50.00	1.63x	7.2%

AI EXPLANATION

Anomalous behavior detected:
• Process Creation is significantly elevated (5.1x baseline, 21.6% contribution)
• Failed Logins is significantly elevated (2.7x baseline, 13.5% contribution)
• Network In is significantly elevated (2.4x baseline, 11.8% contribution)

■■ Possible brute force attack or credential stuffing attempt

RECOMMENDED ACTIONS

1. Isolate the affected endpoint from the network immediately
2. Conduct a forensic analysis of the endpoint
3. Review and analyze related logs for the affected timeframe
4. Check for lateral movement to other systems
5. Update detection rules based on this incident
6. Implement recommended MITRE ATT&CK; mitigations