SECURITY INCIDENT REPORT

Incident ID:	INC-3432AD
Severity:	CRITICAL
Status:	OPEN
Detection Time:	2026-02-01 21:00:32 UTC
Endpoint:	EP-0071
Attack Type:	privilege_escalation

Report Generated: 2026-02-01 21:00:36

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0071** at 2026-02-01 21:00:32 UTC. The anomaly detection system identified suspicious behavior with an ensemble confidence of **95.0%**.

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

Current Status: **OPEN**
Severity Classification: **CRITICAL**

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	1.000
Isolation Forest	0.728
LOF	1.000
Ensemble	**0.909**
Confidence	**95.0%**

MITRE ATT&CK; TECHNIQUES

T1021: Remote Services

Tactic: Lateral Movement
Confidence: 95.0%
Matched Features: process_creation
Description: Adversaries may use valid accounts to log into a service specifically designed to accept remote connections.

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.

T1068: Exploitation for Privilege Escalation

Tactic: Privilege Escalation
Confidence: 67.2%

Matched Features: process_creation, api_calls, memory_usage
Description: Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Process Creation	52.49	5.00	10.50x	24.2%
Failed Logins	0.00	0.50	0.00x	23.6%
Api Calls	295.35	100.00	2.95x	11.4%
Memory Usage	100.00	45.00	2.22x	8.6%
Disk Write	36.73	100.00	0.37x	7.8%
Disk Read	79.06	200.00	0.40x	7.2%
File Access	94.99	50.00	1.90x	7.1%

AI EXPLANATION

Anomalous behavior detected:
• Process Creation is significantly elevated (10.5x baseline, 24.2% contribution)
• Failed Logins is significantly reduced (0.0x baseline, 23.6% contribution)
• Api Calls is significantly elevated (3.0x baseline, 11.4% contribution)

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