




 elastic / **detection-rules** Public


 Notifications


 Fork **498**


 Star **2k**


 **Code**


 Issues **145**


 Pull requests **19**



 Actions


 Security

 Insights

detection-rules / rules / integrations / aws / initial_access_via_system_manager.toml 








 **shashank-elastic** Back-porting Version Trimming ([#3704](#)) 

63e91c2 · 5 months ago 

114 lines (95 loc) · 5.96 KB

Code Blame

Raw     

```
1  [metadata]
2  creation_date = "2020/07/06"
3  integration = ["aws"]
4  maturity = "production"
5  updated_date = "2024/05/21"
6
7  [rule]
8  author = ["Elastic"]
9  description = ""
10 Identifies the execution of commands and scripts via System Manager. Execution methods such as RunS
11 RunPowerShellScript, and alike can be abused by an authenticated attacker to install a backdoor or
12 compromised instance via reverse-shell using system only commands.
13 ""
14 false_positives = [
15     ""
16     Verify whether the user identity, user agent, and/or hostname should be making changes in your
17     Suspicious commands from unfamiliar users or hosts should be investigated. If known behavior is
18     positives, it can be exempted from the rule.
19     "",
20 ]
21 from = "now-60m"
22 index = ["filebeat-*", "logs-aws.cloudtrail-*"]
23 interval = "10m"
24 language = "kuery"
25 license = "Elastic License v2"
26 name = "AWS Execution via System Manager"
```

```
27     note = """"## Triage and analysis
28
29     ### Investigating AWS Execution via System Manager
30
31     Amazon EC2 Systems Manager is a management service designed to help users automatically collect software
32
33     This rule looks for the execution of commands and scripts using System Manager. Note that the actual
34
35     ##### Possible investigation steps
36
37     - Identify the user account that performed the action and whether it should perform this kind of action
38     - Investigate other alerts associated with the user account during the past 48 hours.
39     - Validate that the activity is not related to planned patches, updates, network administrator actions
40     - Investigate the commands or scripts using host-level visibility.
41     - Considering the source IP address and geolocation of the user who issued the command:
42         - Do they look normal for the calling user?
43         - If the source is an EC2 IP address, is it associated with an EC2 instance in one of your accounts?
44         - If it is an authorized EC2 instance, is the activity associated with normal behavior for the instance?
45     - Assess whether this behavior is prevalent in the environment by looking for similar occurrences in other
46     - Contact the account owner and confirm whether they are aware of this activity.
47     - Check if this operation was approved and performed according to the organization's change management
48     - If you suspect the account has been compromised, scope potentially compromised assets by tracking
49
50     ### False positive analysis
51
52     - If this rule is noisy in your environment due to expected activity, consider adding exceptions –
53
54     ### Response and remediation
55
56     - Initiate the incident response process based on the outcome of the triage.
57     - Disable or limit the account during the investigation and response.
58     - Identify the possible impact of the incident and prioritize accordingly; the following actions can be taken:
59         - Identify the account role in the cloud environment.
60         - Assess the criticality of affected services and servers.
61         - Work with your IT team to identify and minimize the impact on users.
62         - Identify if the attacker is moving laterally and compromising other accounts, servers, or services.
63         - Identify any regulatory or legal ramifications related to this activity.
64     - Investigate credential exposure on systems compromised or used by the attacker to ensure all compromised
65     - Check if unauthorized new users were created, remove unauthorized new accounts, and request password
66     - Consider enabling multi-factor authentication for users.
67     - Review the permissions assigned to the implicated user to ensure that the least privilege principle
68     - Implement security best practices [outlined](https://aws.amazon.com/premiumsupport/knowledge-center/secure-ec2-instances/)
69     - Take the actions needed to return affected systems, data, or services to their normal operational state
70     - Identify the initial vector abused by the attacker and take action to prevent reinfection via the same
71     - Using the incident response data, update logging and audit policies to improve the mean time to detect
72
```

```
73     ## Setup
74
75     The AWS Fleet integration, Filebeat module, or similarly structured data is required to be compatible
76     references = ["https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-plugins.html"]
77     risk_score = 21
78     rule_id = "37b211e8-4e2f-440f-86d8-06cc8f158cfa"
79     severity = "low"
80     tags = [
81         "Domain: Cloud",
82         "Data Source: AWS",
83         "Data Source: Amazon Web Services",
84         "Data Source: AWS SSM",
85         "Use Case: Log Auditing",
86         "Tactic: Initial Access",
87         "Resources: Investigation Guide",
88     ]
89     timestamp_override = "event.ingested"
90     type = "query"
91
92     query = '''
93     event.dataset:aws.cloudtrail and event.provider:ssm.amazonaws.com and event.action:SendCommand and
94     '''
95
96
97     [[rule.threat]]
98     framework = "MITRE ATT&CK"
99     [[rule.threat.technique]]
100     id = "T1566"
101     name = "Phishing"
102     reference = "https://attack.mitre.org/techniques/T1566/"
103     [[rule.threat.technique.subtechnique]]
104     id = "T1566.002"
105     name = "Spearphishing Link"
106     reference = "https://attack.mitre.org/techniques/T1566/002/"
107
108
109
110     [rule.threat.tactic]
111     id = "TA0001"
112     name = "Initial Access"
113     reference = "https://attack.mitre.org/tactics/TA0001/"
```