

[New Rule] AWS STS GetSessionToken Abuse #1213

New issue

Merged

w0rk3r merged 34 commits into elastic:main from austinsonger:lateral_movement_sts_getsessiontoken_abuse.toml on Sep 22, 2021

Conversation 8

Commits 34

Checks 0

Files changed

austinsonger commented on May 17, 2021 • edited

Contributor

Issues

Resolves #1152

Relates #955

Summary

Contributor checklist

- Have you signed the contributor license agreement?
- Have you followed the contributor guidelines?

Reviewers

brokensound77

✓

w0rk3r

✓

Assignees

w0rk3r

Labels

backport: auto

community

Domain: Cloud

Integration: AWS

Rule: New

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

✓

[New Rule] AWS STS GetSessionToken Abuse

4 participants

austinsonger and others added 24 commits 3 years ago

Update impact_iam_deactivate_mfa_device.toml

13b7a2c

Update impact_iam_deactivate_mfa_device.toml

da7d230

Update discovery_post_exploitation_external_ip_lookup.toml

b57fd60

Merge branch 'main' into main

b0bddce

Merge branch 'main' into main

178baaf

Update rules/aws/impact_iam_deactivate_mfa_device.toml

475a132

Revert "Update discovery_post_exploitation_external_ip_lookup.toml"

ef40cc2

Merge pull request #1 from elastic/main

3c9fed2

Merge pull request #2 from elastic/main

76344b7

Merge pull request #3 from elastic/main

1f4723e

Merge pull request #4 from elastic/main

e60c7fe

Merge branch 'elastic:main' into main

71b7597

Merge branch 'elastic:main' into main

80d1035

Merge branch 'elastic:main' into main

bdf860d

Merge branch 'elastic:main' into main

d5dda87

Update


6833d0b

New Rule: Okta User Attempted Unauthorized Access

006e02e


Update privilege_escalation_okta_user_attempted_unauthorized_access.toml

1297aac

- 


Update

privilege_escalation_okta_user_attempted_unauthorized_access.toml

7d6357a
- 


Delete

privilege_escalation_okta_user_attempted_unauthorized_access.toml

72ffc88
- 


Create

persistence_new-or-modified-federation-domain.toml


037d240
- 

Delete

persistence_new-or-modified-federation-domain.toml

5bb487b
- 

Merge branch 'elastic:main' into main


0be9c10
- 

Create

lateral_movement_sts_getsessiontoken_abuse.toml

26cd47d

  **github-actions** bot added the **backport: auto** label on May 17, 2021

- 

Rename

lateral_movement_sts_getsessiontoken_abuse.toml to privilege_e... ...

d5cb7ff

  **rw-access** added the **community** label on May 18, 2021

- 

Update

privilege_escalation_sts_getsessiontoken_abuse.toml

5457646

  **brokensound77** added the **Rule: New** label on Jun 15, 2021

  **brokensound77** reviewed on Jun 22, 2021 [View reviewed changes](#)

- .gitignore Outdated Show resolved

rules/aws/privilege_escalation_sts_getsessiontoken_abuse.toml Outdated Show resolved

rules/aws/privilege_escalation_sts_getsessiontoken_abuse.toml Outdated Show resolved

  **brokensound77** requested a review from **bm11100** 3 years ago

 **austinsonger** and others added 6 commits [3 years ago](#)

- 

Update

rules/aws/privilege_escalation_sts_getsessiontoken_abuse.toml

396345d



Update

.gitignore ...

c03ae40



Merge branch 'elastic:main' into

lateral_movement_sts_getsessiontoken... ...

196c1b2



Update

privilege_escalation_sts_getsessiontoken_abuse.toml

370c45d



Update

privilege_escalation_sts_getsessiontoken_abuse.toml

78e9701



Update

5fdf7a8

  **w0rk3r** requested changes on Sep 22, 2021 [View reviewed changes](#)

w0rk3r left a comment Contributor ...

License needs to be added, other than that, LGTM

rules/integrations/aws/privilege_escalation_sts_getsessiontoken_abuse.toml

Outdated

Show resolved

botelasticbot added Domain: Cloud Integration: AWS labels on Sep 22, 2021

w0rk3r self-assigned this on Sep 22, 2021

austinsonger and others added 2 commits 3 years ago

Update

rules/integrations/aws/privilege_escalation_sts_getsessiontoken...

1f2dcf9

Merge branch 'main' into lateral_movement_sts_getsessiontoken_abuse.toml

fbfdfc9

brokensound77 removed the request for review from bm11100 3 years ago

brokensound77 approved these changes on Sep 22, 2021

View reviewed changes

brokensound77 left a comment

Contributor

...

LGTM, thanks

w0rk3r approved these changes on Sep 22, 2021

View reviewed changes

w0rk3r merged commit 93b8038 into elastic:main on Sep 22, 2021

protectionsmachine pushed a commit that referenced this pull request on Sep 22, 2021

[New Rule] AWS STS GetSessionToken Abuse (#1213)

...

03ac44e

protectionsmachine pushed a commit that referenced this pull request on Sep 22, 2021

[New Rule] AWS STS GetSessionToken Abuse (#1213)

...

216d06e

protectionsmachine pushed a commit that referenced this pull request on Sep 22, 2021

[New Rule] AWS STS GetSessionToken Abuse (#1213)

...

914db6a

austinsonger deleted the lateral_movement_sts_getsessiontoken_abuse.toml branch 3 years ago

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)