



elastic / **detection-rules** Public

Notifications

Fork 498

Star 2k

<> Code

Issues 145

Pull requests 19

Actions

Security

Insights

[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 • Contributor

edited

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

austinsonger and others added 24 commits 3 years ago











Update



Verified


13b7a2e

impact_iam_deactivate_mfa_device.toml

...		
Update	Verified	da7d230
impact_iam_deactivate_mfa_device.toml		Development
Update	Verified	b57fd60
discovery_post_exploitation_external_ip_lookup.toml		Successfully merging this pull request may close these issues.
...		[New Rule] AWS STS GetSessionToken Ab...
Merge branch 'main' into main	Verified	b0bddce 4 participants
Merge branch 'main' into main	Verified	178baaf
Update	Verified	475a132
rules/aws/impact_iam_deactivate_mfa_device.toml		
...		
Revert "Update		ef40cc2
discovery_post_exploitation_external_ip_lookup.toml"		
...		
Merge pull request #1 from elastic/main	Verified	3c9fed2
Merge pull request #2 from elastic/main	Verified	76344b7
Merge pull request #3 from elastic/main	Verified	1f4723e
Merge pull request #4 from elastic/main	Verified	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	Verified	1297aac
privilege_escalation_okta_user_attempted_unauthorized_access.toml		
Update	Verified	7d6357a
privilege_escalation_okta_user_attempted_unauthorized_access.toml		

-   Delete Verified 72ffc88
privilege_escalation_okta_user_attempted_unauthorized_access.toml
-   Create persistence_new-or- Verified 037d240
modified-federation-domain.toml
-   Delete persistence_new-or- Verified 5bb487b
modified-federation-domain.toml
-   Merge branch 'elastic:main' into main 0be9c10
-   Create Verified 26cd47d
lateral_movement_sts_getsessiontoken_abuse.toml

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

-   Rename Verified d5cb7ff
lateral_movement_sts_getsessiontoken_abuse.toml
to privilege_e... 

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


-   Update Verified 5457646
privilege_escalation_sts_getsessiontoken_abuse.toml


  **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 Verified 396345d
rules/aws/privilege_escalation_sts_getsessiontoken_abuse.toml
...

  Update .gitignore ... Verified c03ae40

  Merge branch 'elastic:main' into Verified 196c1b2
lateral_movement_sts_getsessiontoken...
...

  Update Verified 370c45d
privilege_escalation_sts_getsessiontoken_abuse.toml

  Update 78e9701
privilege_escalation_sts_getsessiontoken_abuse.toml


  Update 5fdf7a8





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

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



  **botelastic** bot 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  1f2dcf9
rules/integrations/aws/privilege_escalation_sts_getsessiontoke...

  Merge branch 'main' into  fbfdcf9
lateral_movement_sts_getsessiontoken_abuse.toml

  brokensound77 removed the request for review from
bm11100 3 years ago




 brokensound77 approved these [View reviewed changes](#)
changes on Sep 22, 2021



brokensound77 left a comment


[Contributor](#) ...

LGTM, thanks




 w0rk3r approved these changes [View reviewed changes](#)
on Sep 22, 2021

  w0rk3r merged commit **93b8038** into [elastic:main](#)
on Sep 22, 2021

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

  [New Rule] AWS STS GetSessionToken Abuse  03ac44e
([#1213](#)) ...

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


  [New Rule] AWS STS GetSessionToken Abuse  216d06e
([#1213](#)) ...



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

 [New Rule] AWS STS GetSessionToken Abuse 914db6a (#1213) ...



 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](#)