




[New Rule] AWS STS AssumeRole Usage #1214


New issue


 Merged


w0rk3r merged 49 commits into elastic:main from austinsonger:lateral_movement_sts_assumerole_abuse.toml


 on Oct 15, 2021

 Conversation 14

 Commits 49

 Checks 0

 Files changed



austinsonger commented on May 17, 2021 • edited ▼

Contributor

...

Issues


Resolves [#1153](#)
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 AssumeRole 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









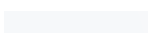


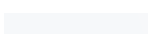






  Merge branch 'elastic:main' into main bdf860d





  Merge branch 'elastic:main' into main d5dda87



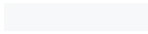
  Update 6833d0b

  New Rule: Okta User Attempted Unauthorized Access 006e02e

  Update privilege_escalation_okta_user_attempted_unauthorized_access.toml 1297aac



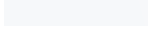



-   Update privilege_escalation_okta_user_attempted_unauthorized_access.toml  7d6357a
-   Delete privilege_escalation_okta_user_attempted_unauthorized_access.toml  72ffc88
-   Create persistence_new-or-modified-federation-domain.toml  037d240
-   Delete persistence_new-or-modified-federation-domain.toml  5bb487b
-   Merge branch 'elastic:main' into main  0be9c10
-   Create lateral_movement_sts_assumerole_abuse.toml  cb22759


  **github-actions**  added the  label on May 17, 2021

-   Rename lateral_movement_sts_assumerole_abuse.toml to privilege_escala...  3d8fdda

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

 **austinsonger** added 2 commits [3 years ago](#)

-   Merge branch 'main' into lateral_movement_sts_assumerole_abuse.toml  1fdfa63
-   Update privilege_escalation_sts_assumerole_abuse.toml  97ceeca



austinsonger commented on Jun 2, 2021 • edited

Contributor



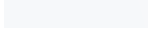





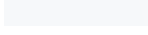
Author

...

@bm11100 I was thinking about something you commented on another [issue](#). This one could be noisy because of Terraform as well. So I added a false positive.






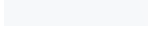
12 hidden items
[Load more...](#)

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

-   Update privilege_escalation_sts_assumerole_abuse.toml  1c4beb1
-   Update privilege_escalation_sts_assumerole_abuse.toml  8795e85
-   Update and rename privilege_escalation_sts_assumerole_abuse.toml to p...  4101281

  **austinsonger** changed the title ~~[New Rule] AWS STS AssumeRole Abuse~~ **[New Rule] AWS STS AssumeRole Usage** on Oct 6, 2021

 **austinsonger** added 2 commits [3 years ago](#)

-   Merge branch 'main' into lateral_movement_sts_assumerole_abuse.toml  60657e4
-   Merge branch 'main' into lateral_movement_sts_assumerole_abuse.toml  f3dfc91



 **w0rk3r** approved these changes on Oct 11, 2021

[View reviewed changes](#)

w0rk3r left a comment

Contributor

...

LGTM

w0rk3r requested a review from **brokensound77** 3 years ago

w0rk3r requested changes on Oct 11, 2021

View reviewed changes

rules/integrations/aws/privilege_escalation_sts_assumerole_usage.toml

Show resolved

austinsonger and others added 2 commits 3 years ago

Update

rules/integrations/aws/privilege_escalation_sts_assumerole_usa...

17ebc52

Add note field

746fbf3

w0rk3r approved these changes on Oct 11, 2021

View reviewed changes

brokensound77 reviewed on Oct 12, 2021

View reviewed changes

rules/integrations/aws/privilege_escalation_sts_assumerole_usage.toml

Outdated

Show resolved

austinsonger added 2 commits 3 years ago

Update privilege_escalation_sts_assumerole_usage.toml

073166c

Merge branch 'main' into lateral_movement_sts_assumerole_abuse.toml

85b020d

w0rk3r reviewed on Oct 12, 2021

View reviewed changes

rules/integrations/aws/privilege_escalation_sts_assumerole_usage.toml

Outdated

Show resolved

austinsonger and others added 2 commits 3 years ago

Update

rules/integrations/aws/privilege_escalation_sts_assumerole_usa...

dc79680

Merge branch 'main' into lateral_movement_sts_assumerole_abuse.toml

d796269

w0rk3r requested a review from **brokensound77** 3 years ago

Merge branch 'main' into lateral_movement_sts_assumerole_abuse.toml

083387e

brokensound77 reviewed on Oct 15, 2021

View reviewed changes

rules/integrations/aws/privilege_escalation_sts_assumerole_usage.toml

Outdated

18 + index = ["filebeat-*", "logs-aws*"]

19 + language = "kuery"

20 + license = "Elastic License v2"

21 + name = "AWS STS AssumeRole Usage"

brokensound77 on Oct 15, 2021


Contributor

...

Page 3 of 4

can we expand STS


Also are there references to add?

 w0rk3r on Oct 15, 2021

Contributor

...


@brokensound77 does these changes solve this one?

 brokensound77 on Oct 15, 2021

Contributor

...

👍 LGTM



✔

brokensound77 approved these changes on Oct 15, 2021

View reviewed changes

brokensound77 left a comment

Contributor

...

After the remaining comment is resolved, then this LGTM 👍



w0rk3r added 3 commits 3 years ago



 Adding Reference

0d10f39



 Expand STS

d542b9f



 Merge branch 'main' into lateral_movement_sts_assumerole_abuse.toml

5123fa7



 w0rk3r merged commit d7eab5b into elastic:main on Oct 15, 2021




protectionsmachine pushed a commit that referenced this pull request on Oct 15, 2021



 [New Rule] AWS STS AssumeRole Usage (#1214)

...

72e7747



protectionsmachine pushed a commit that referenced this pull request on Oct 15, 2021



 [New Rule] AWS STS AssumeRole Usage (#1214)


...

25733e1



protectionsmachine pushed a commit that referenced this pull request on Oct 15, 2021



 [New Rule] AWS STS AssumeRole Usage (#1214)

...

3242cdb



 austinsonger deleted the lateral_movement_sts_assumerole_abuse.toml branch 3 years ago

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