



elastic / detection-rules Public

Notifications Fork 498 Star 2k

<> Code Issues 145 Pull requests 19 Actions Security Insights

[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 • Contributor

edited

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

austinsonger and others added 24 commits 3 years ago

Update











impact\_iam\_deactivate\_mfa\_device.toml

Verified

13b7a2f Milestone

No milestone

	Update	Verified	da7d230	Development
	impact_iam_deactivate_mfa_device.toml			
	Update	Verified	557fd60	These issues
	discovery_post_exploitation_external_ip_lookup.toml			
	...			[New Rule] AWS STS AssumeRole Abuse
	Merge branch 'main' into main	Verified	b0bddce	
	Merge branch 'main' into main	Verified	178baaf	4 participants
	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	Verified	3c9fed2	
	elastic/main			
	Merge pull request #2 from	Verified	76344b7	
	elastic/main			
	Merge pull request #3 from	Verified	1f4723e	
	elastic/main			
	Merge pull request #4 from	Verified	e60c7fe	
	elastic/main			
	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		006e02e	
	Access			
	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-modified-federation-domain.toml Verified 037d240
-  Delete persistence\_new-or-modified-federation-domain.toml Verified 5bb487b
-  Merge branch 'elastic:main' into main 0be9c10
-  Create lateral\_movement\_sts\_assumerole\_abuse.toml Verified cb22759
-  github-actions bot added the backport: auto label on May 17, 2021
-  Rename lateral\_movement\_sts\_assumerole\_abuse.toml to privilege\_escalation\_sts\_assumerole\_abuse.toml Verified 3d8fdda
-  rw-access added the community label on May 18, 2021
-  austinsonger added 2 commits 3 years ago
-  Merge branch 'main' into lateral\_movement\_sts\_assumerole\_abuse.toml Verified 1fdfa63
-  Update privilege\_escalation\_sts\_assumerole\_abuse.toml Verified 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 Verified 1c4beb1  
privilege\_escalation\_sts\_assumerole\_abuse.toml
  -   Update Verified 8795e85  
privilege\_escalation\_sts\_assumerole\_abuse.toml
  -   Update and rename Verified 4101281  
privilege\_escalation\_sts\_assumerole\_abuse.toml  
to p... 

  **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  60657e4  
lateral\_movement\_sts\_assumerole\_abuse.toml
  -   Merge branch 'main' into  f3dfc91  
lateral\_movement\_sts\_assumerole\_abuse.toml



 **w0rk3r** approved these changes [View reviewed changes](#) on Oct 11, 2021

**w0rk3r** left a comment

Contributor 


LGTM



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





 **w0rk3r** requested changes [View reviewed changes](#) on Oct 11, 2021

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...  
...



 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...  
...



 Merge branch 'main' into  
lateral\_movement\_sts\_assumerole\_abuse.toml  
d796269

 w0rk3r requested a review from brokenound77 3 years ago

  Merge branch 'main' into  083387e  
lateral\_movement\_sts\_assumerole\_abuse.toml

 brokenound77 reviewed [View reviewed changes](#)  
on Oct 15, 2021

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"
```

 brokenound77 on Oct 15, 2021 Contributor ...

can we expand STS


Also are there references to add?

 w0rk3r on Oct 15, 2021 Contributor ...

[@brokenound77](#) does these changes solve this one?

 brokenound77 on Oct 15, 2021 Contributor ...

👍 LGTM


 brokenound77 approved these [View reviewed changes](#)  
changes on Oct 15, 2021











brokenound77 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 72e7747 (#1214) ...
-  protectionsmachine pushed a commit that referenced this pull request on Oct 15, 2021
  -   [New Rule] AWS STS AssumeRole Usage 25733e1 (#1214) ...
-  protectionsmachine pushed a commit that referenced this pull request on Oct 15, 2021
  -   [New Rule] AWS STS AssumeRole Usage 3242cdb (#1214) ...
-   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](#)

