Share:

State	Resolved (Closed)
Disclosed	**July 18, 2019 8:57pm +0530**
Reported To	Chainlink
Asset	https://chain.link/ (Domain)
Weakness	Improper Authentication - Generic
Bounty	$500
Severity	Medium (4 ~ 6.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE

danangtriatmaja submitted a report to **Chainlink**. Jun 25th (24 days ago)

Hiii,

There is any issue No valid SPF Records

Desciprition :

There is a email spoofing vulnerability.Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.

I found :

SPF record lookup and validation for: chain.link
SPF records are published in DNS as TXT records.

The TXT records found for your domain are:
google-site-verification=a4ghJBW7o-Ss_TB82G2VqvQKq_8Km3UfqcuTgfc8ISY
v=spf1 include:_spf.google.com ~all

Checking to see if there is a valid SPF record.

Found v=spf1 record for chain.link:
v=spf1 include:_spf.google.com ~all

evaluating...
SPF record passed validation test with pySPF (Python SPF library)!

Use the back button on your browser to return to the SPF checking tool without clearing the form.

Remediation :

Replace ~all with -all to prevent fake email.

Refferences :

https://www.digitalocean.com/community/tutorials/how-to-use-an-spf-record-to-prevent-spoofing-improve-e-mail-reliability

Impact

An attacker would send a Fake email. The results can be more dangerous.

1 attachment:
F516445: chain.png

thodges changed the status to ○ **Needs more info**. Jun 25th (24 days ago)
Thank you for the report @danangtriatmaja, however, we have received this report several times previously. I do not believe that the difference between `~all` and `-all` constitutes a Medium severity. We have also had other hackers test to make sure that fake emails cannot be sent. If you can actually forge an email to thomas@smartcontract.com coming from the chain.link domain, I'll reconsider.

danangtriatmaja changed the status to ○ **New**. Jun 25th (24 days ago)
For now, according to my knowledge it's better to use -all than ~all in terms of security and I have a POC from impacts that can be caused

1 attachment:
F516497: spfrecord-impact.mp4

thodges changed the status to ○ **Needs more info**. Jun 25th (24 days ago)
@danangtriatmaja Your video shows a POC when there is no SPF record present, which has been fixed on our chain.link domain. I want you to prove that you can still forge emails with the current setting of `~all`, since that is what you are reporting as a vulnerability.

danangtriatmaja changed the status to ○ **New**. Jul 3rd (16 days ago)
Ill try to create a video for PoC, the case in chain.link :

1 attachment:
F521340: chain-2019-07-03_02.08.36.mp4

thodges changed the status to ○ **Triaged**. Jul 4th (15 days ago)
@danangtriatmaja Perfect! This is exactly what we thought was previously resolved. Thank you!

Chainlink rewarded danangtriatmaja with a **$500** bounty. Jul 4th (15 days ago)
Thank you @danangtriatmaja!

danangtriatmaja posted a comment. Jul 4th (15 days ago)
Hi @chainlink

Thanks for the bounties

Cheers

danangtriatmaja posted a comment. Jul 4th (15 days ago)
Can we dislcose this one ?

thodges posted a comment. Jul 4th (15 days ago)
Let's wait until resolved, please.

danangtriatmaja posted a comment. Jul 15th (4 days ago)
Any update for this report ? when im review the report, it has been fixed :)

thodges closed the report and changed the status to ○ **Resolved**. Jul 18th (about 1 day ago)
Thank you @danangtriatmaja this is indeed resolved now!

thodges requested to disclose this report. Jul 18th (about 1 day ago)

danangtriatmaja agreed to disclose this report. Jul 18th (15 hrs ago)

Thanks

This report has been disclosed. Jul 18th (15 hrs ago)