"Bounties paid in the last 90 days" discloses the undisclosed bounty amount in program statistics

73

Share:

State	Resolved (Closed)
Disclosed	**February 22, 2020 12:43am +0530**
Reported To	HackerOne
Asset	https://hackerone.com (Domain)
Weakness	Information Disclosure
Bounty	$500
Severity	Low (3.8)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

japz submitted a report to **HackerOne**. Sep 17th (9 months ago)

Hi Team,

Summary:

I have found a bypass on this disclosed report: Know undisclosed Bounty Amount when Bounty Statistics are enabled.

Description:

When a program does not disclose how much bounty is paid to particular report, but if bounty statics is enabled then undisclosed Bounty Amount can be enumerated using the **"Bounties paid in the last 90 days".**

"Bounties paid in the last 90 days" is the total amount paid in the last 90 days, so by doing a basic mathematical equation, we can be able to determine the undisclosed bounty amount, below is the formula to get the undisclosed bounty amount.

Formula

`old` = `Old Bounties paid in the last 90 days` >> Total 90 days bounty paid
`new` = `New Bounties paid in the last 90 days` >> Everytime the 90 days bounty changes

`undisclosed amount` = `old - new`

Mitigation:

Use the same fix you have applied in this report #148050

Impact

Disclosing the undisclosed bounty amount for program which is not disclosing bounties in their settings.

Let me know if anything else is needed.

Regards
Japz

sodacan HackerOne triage posted a comment. Sep 18th (9 months ago)

Hi @japz,

Thank you for your submission. Your report is currently being reviewed and the HackerOne triage team will get back to you once there is additional information to share.

Kind regards,
@sodacan

japz posted a comment. Sep 23rd (8 months ago)

Hi @sodacan ,

It's almost a week now, any updates from the triage team ?

Regards
Japz

japz posted a comment. Updated Feb 22nd (3 months ago)
If you need additional proof:

I can comment that [redacted] was recently rewarded (2 days ago) with `$550` dollars by [redacted] private program.

It's because [redacted] `Bounties paid in the last 90 days` last week is `$1,750` and last 2 days it changes to `$2,300`.

So `$2,300` - `$1,750` = `$550`

[redacted]

Regards
Japz

japz posted a comment. Sep 27th (8 months ago)
Hi @sodacan ,

Do we have any updates on this ?

Regards
Japz

sodacan HackerOne triage posted a comment. Sep 27th (8 months ago)
Hi @japz,
No updates are available yet. We will be sure to let you know when that changes.
@sodacan

japz posted a comment. Sep 30th (8 months ago)

pei HackerOne staff changed the status to ○ **Triaged**. Sep 30th (8 months ago)
Hi @japz - Thanks for the report! I've triaged this and will escalate it to one of our teams.

japz posted a comment. Oct 1st (8 months ago)
Thanks @pei - Please keep me updated. Regards

japz posted a comment. Updated Oct 7th (8 months ago)
Hi @pei,

It's almost a week now, do we have any updates on this ?

Regards
Japz

bencode HackerOne staff posted a comment. Oct 10th (8 months ago)
Hey @japz,

We're still reviewing, we'll make a bounty decision this Friday. Thanks for your patience.

@bencode

jobert HackerOne staff updated the severity from Low to Low (3.8). Oct 11th (8 months ago)

HackerOne rewarded japz with a **$500** bounty. Oct 11th (8 months ago)
Thanks @japz, good find. We'll get back to you once we've pushed a fix for this. Enjoy your weekend!

japz posted a comment. Oct 11th (8 months ago)
Hi @jobert / Team,

> We'll get back to you once we've pushed a fix for this. Enjoy your weekend!

Noted, thanks for the bounty.. much appreciated. Enjoy your weekend too. :)

Cheers
Japz

pei HackerOne staff posted a comment. Oct 29th (7 months ago)
hi @japz - our engineering team has pushed out a fix. could you please verify? thanks!

japz posted a comment. Oct 30th (7 months ago)
Hi @pei ,

Can you give me a little info of what kind of fix they did ? , so that i can verify. Because i cannot see any changes from the response.

Thanks
Japz

pei HackerOne staff posted a comment. Oct 30th (7 months ago)
Seems like the team decided to be consistent with how we handled the total bounties and did the approximation for 90 days as well.

japz posted a comment. Nov 4th (7 months ago)
Hi @pei ,

> Seems like the team decided to be consistent with how we handled the total bounties and did the approximation for 90 days as well.

If that is the case, i believe the approximation for 90 days is enough. You guys can verify it yourself since i cannot query the exact total for any of the existing program.

You can close if you believe the approximation is already in place.

Regards
Japz

jobert HackerOne staff closed the report and changed the status to ○ **Resolved**. Feb 14th (4 months ago)
Hi @japz - thanks again for bringing this to our attention! This report was lingering in our Triage queue. We believe the approximation is OK, so we'll mark this as Resolved. Looking forward to receiving more reports from you :) Good luck and happy hacking!

japz requested to disclose this report. Feb 16th (3 months ago)

jobert HackerOne staff agreed to disclose this report. Feb 22nd (3 months ago)

This report has been disclosed. Feb 22nd (3 months ago)