

# Forum:[Hack Forums](#)

Thread: [Microsoft Launches \\$5M Bug Bounty in Latest Zero Day Quest](#)

JoseMar - August 6, 2025, 12:15 am

## Microsoft Launches \$5M Bug Bounty in Latest Zero Day Quest

### The Bounty Hits 5 Million

Alright, so here's something that might catch your attention if you're even remotely into bug hunting or just watching tech giants squirm a bit under the pressure of their own systems.

Microsoft just dropped news of their latest Zero Day Quest. Yes, it's exactly what it sounds like: a high-stakes, global bug bounty program. The prize pool? Up to five million dollars. Yeah, with six zeroes. That's not a typo or a clickbait headline, five million real-world, government-backed dollars for digging into their systems.

If you're thinking, "That sounds... aggressive," you're not alone.

Last year, they had a similar thing and capped it at 4 million. This year, they're basically saying, "Alright, let's go even harder." Feels a bit like they're raising the stakes because they know they have to.

### Not Just A PR Move (Probably)

Now, here's where it gets interesting. Microsoft isn't just throwing money around for attention. Well, maybe a little. But there's strategy behind this.

They're focusing on what they call a "collaborative defense" model, which basically means, instead of waiting for things to blow up (like, say, a critical Azure exploit making headlines), they're paying smart folks before it happens.

So yeah, instead of reacting to chaos, they're trying to pre-buy peace. Crowdsourcing safety, in a way. It's kind of clever. Or desperate. Or both. But still, better than nothing.

### What They're Letting You Hack

They've narrowed in on some pretty sensitive real estate. Here's the shortlist: Azure (everyone's cloud everything)

- Copilot (their shiny AI assistant thing)

- Microsoft 365

- Dynamics 365

- Identity Services

- Power Platform

Basically, all the stuff that businesses use, and hackers love.

They didn't pick those at random, either. MSRC (their security team) publicly said these are high priority because they're widely adopted and, if breached, would have cascading effects.

So if you've ever looked at Copilot and thought, "I wonder what's under the hood?", now might be a good time to take a peek (legally).

#### Double Points for the Brave

There's a twist: for the first 60 days (Aug 4 to Oct 4, 2025), they're offering 50% bonus payouts for high-severity findings.

So if you find something truly nasty, say, a critical auth bypass on Azure, you're not just getting paid. You're getting paid paid.

This two-phase structure is intentional. It kind of gamifies the whole thing. If you're early and good, you win big. If you're late or sloppy... well, maybe next time.

Also, all this has to go through their Coordinated Vulnerability Disclosure framework. Which makes sense. No one wants to see an RCE dropped on GitHub the morning of patch Tuesday.

#### What This Says About the Bigger Picture

Zooming out a bit, this is kind of a snapshot of where we're headed with cybersecurity.

The attack surface is expanding fast (AI, cloud, identity systems, you name it). Traditional in-house red teams just can't cover everything anymore. So companies like Microsoft are leaning into external talent. Bug bounty as infrastructure, almost.

Sure, it's a little scary that they're this eager to hand over millions for help. But also... maybe that's how security gets better now. Not with locked doors, but open invitations.

That said, if I were a black hat with zero scruples, I'd be looking at this and thinking: "Five million here, or ten million under the table from someone else?" So yeah. That tension's not going away.

#### Not a Mic Drop

Anyway, if you're the kind of person who likes poking at systems, or you know someone who is, this might be worth looking into.

The Zero Day Quest isn't just a cash grab. It's Microsoft's way of admitting they can't win this alone.

And maybe that's the part I find most human about all of it.

So, [Mooooookie](#), what do you think about this? This is not like this when they win just 8k [Chrome Users: One Click Away from Full System Compromise \(CVE-2025-8292\)](#)

I'll tag some skilled hackers here to check when they're available.

[6](#)  
[Bastille](#)  
[Money-](#)  
[Tor](#)  
[CL1B](#)  
[skull](#)  
[DramaKing](#)

I can't tag everyone, so feel free to spread the word!

Here's the article I found with the details:

<https://msrc.microsoft.com/blog/2025/08/zero-day-quest-join-the-largest-hacking-event-with-up-to-5-million-in-total-bounty-awards/>

You can submit it here: <https://msrc.microsoft.com/report/vulnerability/new>

**CL1B** - August 6, 2025, 1:46 am

Quite the bug bounty program. I wish everyone good luck in their attempts/research.

Spoiler ([Click to View](#)) Remember to always be discrete and always use their CVD program

**Chornaya Magiya** - August 6, 2025, 5:43 am

Please share url where to submit bug bounties want to review more detailed, i have a lot of o365 exploits and tricks , maybe some of them are worth \$\$ now

??????????? - August 6, 2025, 6:17 am

(Aug 6, 2025 12:15 AM)JoseMar Wrote: ([CITE](#)) Microsoft Launches \$5M Bug Bounty in Latest Zero Day Quest

The Bounty Hits 5 Million

Alright, so here's something that might catch your attention if you're even remotely into bug hunting or just watching tech giants squirm a bit under the pressure of their own systems.

Microsoft just dropped news of their latest Zero Day Quest. Yes, it's exactly what it sounds like: a high-stakes, global bug bounty program. The prize pool? Up to five million dollars. Yeah, with six zeroes. That's not a typo or a clickbait headline, five million real-world, government-backed dollars for digging into their systems.

If you're thinking, "That sounds... aggressive," you're not alone.

Last year, they had a similar thing and capped it at 4 million. This year, they're basically saying, "Alright, let's go even harder." Feels a bit like they're raising the stakes because they know they have to.

Not Just A PR Move (Probably)

Now, here's where it gets interesting. Microsoft isn't just throwing money around for attention. Well, maybe a little. But there's strategy behind this.

They're focusing on what they call a "collaborative defense" model, which basically means, instead of waiting for things to blow up (like, say, a critical Azure exploit making headlines), they're paying smart folks before it happens.

So yeah, instead of reacting to chaos, they're trying to pre-buy peace. Crowdsourcing safety, in a way. It's kind of clever. Or desperate. Or both. But still, better than nothing.

## What They're Letting You Hack

They've narrowed in on some pretty sensitive real estate. Here's the shortlist: Azure (everyone's cloud everything)

Copilot (their shiny AI assistant thing)

Microsoft 365

Dynamics 365

Identity Services

Power Platform

Basically, all the stuff that businesses use, and hackers love.

They didn't pick those at random, either. MSRC (their security team) publicly said these are high priority because they're widely adopted and, if breached, would have cascading effects.

So if you've ever looked at Copilot and thought, "I wonder what's under the hood?", now might be a good time to take a peek (legally).

## Double Points for the Brave

There's a twist: for the first 60 days (Aug 4 to Oct 4, 2025), they're offering 50% bonus payouts for high-severity findings.

So if you find something truly nasty, say, a critical auth bypass on Azure, you're not just getting paid. You're getting paid paid.

This two-phase structure is intentional. It kind of gamifies the whole thing. If you're early and good, you win big. If you're late or sloppy... well, maybe next time.

Also, all this has to go through their Coordinated Vulnerability Disclosure framework. Which makes sense. No one wants to see an RCE dropped on GitHub the morning of patch Tuesday.

## What This Says About the Bigger Picture

Zooming out a bit, this is kind of a snapshot of where we're headed with cybersecurity.

The attack surface is expanding fast (AI, cloud, identity systems, you name it). Traditional in-house red teams just can't cover everything anymore. So companies like Microsoft are leaning into external talent. Bug bounty as infrastructure, almost.

Sure, it's a little scary that they're this eager to hand over millions for help. But also... maybe that's how security gets better now. Not with locked doors, but open invitations.

That said, if I were a black hat with zero scruples, I'd be looking at this and thinking: "Five million here, or ten million under the table from someone else?" So yeah. That tension's not going away.

## Not a Mic Drop

Anyway, if you're the kind of person who likes poking at systems, or you know someone who is, this might be worth looking into.

The Zero Day Quest isn't just a cash grab. It's Microsoft's way of admitting they can't win this alone.

And maybe that's the part I find most human about all of it.

So, [Mooooookie](#) , what do you think about this? This is not like this when they win just 8k [Chrome Users: One Click Away from Full System Compromise \(CVE-2025-8292\)](#)

I'll tag some skilled hackers here to check when they're available.

[6](#)  
[Bastille](#)  
[Money-](#)  
[Tor](#)  
[CL1B](#)  
[skull](#)  
[DramaKing](#)

I can't tag everyone, so feel free to spread the word!

can you share the exact links?

**JoseMar** - August 6, 2025, 6:53 am

(Aug 6, 2025 05:43 AM)Chornaya Magiya Wrote: [\[CITE\]](#) Please share url where to submit bug bounties want to review more detailed, i have a lot of o365 exploits and tricks , maybe some of them are worth \$\$ now

(Aug 6, 2025 06:17 AM)??????? Wrote: [\[CITE\]](#) can you share the exact links?

Here's the article I found with the details:

<https://msrc.microsoft.com/blog/2025/08/zero-day-quest-join-the-largest-hacking-event-with-up-to-5-million-in-total-bounty-awards/>

You can submit it here:<https://msrc.microsoft.com/report/vulnerability/new>

???????????? - August 6, 2025, 6:56 am

(Aug 6, 2025 06:53 AM)JoseMar Wrote: [\[CITE\]](#) Here's the article I found with the details:

<https://msrc.microsoft.com/blog/2025/08/zero-day-quest-join-the-largest-hacking-event-with-up-to-5-million-in-total-bounty-awards/>

You can submit it here:<https://msrc.microsoft.com/report/vulnerability/new>

Thanks for the link.

**JoseMar** - August 6, 2025, 6:58 am

(Aug 6, 2025 01:46 AM)MarlboroMan Wrote: [\[CITE\]](#) Quite the bug bounty program. I wish everyone good luck in their attempts/research.

Spoiler ([Click to View](#)) Remember to always be discrete and always use their CVD program  
(Aug 6, 2025 05:43 AM)Chornaya Magiya Wrote: [\[CITE\]](#) Please share url where to submit bug bounties want to review more detailed, i have a lot of o365 exploits and tricks , maybe some of them are worth \$\$ now

(Aug 6, 2025 06:56 AM)??????? Wrote: [\[CITE\]](#) Thanks for the link.  
Good luck, and let us know if you find something to report  
??

6 - August 6, 2025, 7:46 am

Sounds great, is it 5M total bounty reward pool?

JoseMar - August 6, 2025, 7:57 am

(Aug 6, 2025 07:46 AM)6 Wrote: [\[CITE\]](#) Sounds great, is it 5M total bounty reward pool?

Yes, refers to the entire prize pool, not per person.

Last year was \$4 million in bounty awards, and this year \$5 million in bounty awards. Go for it ?

0xEIPadrino - August 6, 2025, 9:20 am

(Aug 6, 2025 07:57 AM)JoseMar Wrote: [\[CITE\]](#) Yes, refers to the entire prize pool, not per person.

Last year was \$4 million in bounty awards, and this year \$5 million in bounty awards. Go for it ?

awesome thanks for sharing good luck everyone happy hunting ;)

Mooooookie - August 6, 2025, 12:55 pm

(Aug 6, 2025 12:15 AM)JoseMar Wrote: [\[CITE\]](#) So, [Mooooookie](#) , what do you think about this? This is not like this when they win just 8k[Chrome Users: One Click Away from Full System Compromise \(CVE-2025-8292\)](#)

Shout out to Microsoft for putting their money, where their mouth is. A \$5 million dollar payout could change a persons life.. definitely a motivating reason to go out there and locate weaknesses and bugs within their shit.

If you're going to reward people for helping keep your programs and platform secure, the amount that you're paying them should always be worthwhile.. not only for finding the bug, but as motivation for them to go out and locate more bugs for your company. Bug hunters finding these bugs, before hackers do.. prevents your company in-hindsight from being embarrassed.

Short changing them like Google did, was not, and is not the move.