Microsoft

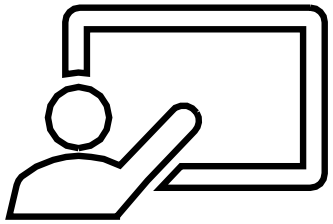
Getting to $10,000

How you can craft your reports for higher impact and bigger bounty awards

Jarek Stanley (@JarekMSFT)
Microsoft Security Response Center

Presented at:

Nullcon
March 1, 2019



Agenda

- Introduction
- Understanding the program
- Crafting high-quality reports
- Program updates

Introduction

The Microsoft bug bounty program rewards security research

Microsoft Office Insider **up to $15K**

Microsoft Edge **up to $15K**

Azure DevOps **up to $20K**

Microsoft Cloud Bounty **up to $20K**

Windows Insider Preview **up to $50K**

Microsoft Identity **up to $100K**

Microsoft Hyper-V **up to $250K**

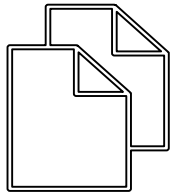
We awarded over US $2 million in 2018

Valuable contribution from India-based researchers

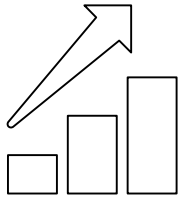
In 2018 alone we awarded US $90,000+ to India-based researchers, 2x increase over 2017.

Four India-based researchers are included in the top 100 security researchers who have contributed research to Microsoft products and service in 2018.

Two keys to increasing success



High-impact reports on high value properties earn higher rewards.



High-quality reports pay off. Show us how to reproduce your findings.

Read the bounty brief to decide what to research

The brief will tell you what we care about and will award. Use it to decide how you should spend your time, energy, and creativity.

`Out of scope = $0`

More info on Microsoft bounty scope: https://www.microsoft.com/en-us/msrc/bounty

Use the STRIDE model to communicate impact

Understand the STRIDE model and use it to communicate impact in your report. It helps us speak the same language.

Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege

Remote Code Execution

https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-threats#stride-model

STRIDE + Severity = 

Cloud Bounty Program Award Structure https://www.microsoft.com/msrc/bounty-microsoft-cloud

Remote code execution	• Critical severity **up to $20,000** • Important severity **up to $15,000**
Elevation of privilege	• Critical severity **up to $8,000** • Important severity **up to $5,000**
Information disclosure	• Critical severity **up to $8,000** • Important severity **up to $5,000**
Spoofing	• No critical severity reports • Important severity **up to $3,000**
Tampering	• No critical severity reports • Important severity **up to $3,000**
Denial of service	• Out of scope for bounty

Higher quality = higher award

Go the extra mile, earn the extra award

Provide clear, concise information about how our engineering teams can **reproduce the vulnerability** for themselves, including version or configuration information where appropriate.

Clear, detailed, well-written instructions, or even short videos **can more than double** the possible award amount for bounty eligible properties.

Offering **attack scenarios, root-cause analysis, and thoughts on potential fixes** can earn even more.

Non-report report – cannot repro

Title:
Your stuff is broken

Description:
Fix your stuff, all of it is broken bro!

Low quality: description only

Title:

Stored XSS at login.microsoftonline.com via OAuth redirect_uri parameter.

Description:

1. Using PUT https://main.iam.ad.ext.azure.com/api/RegisteredApplications/325da240-6a42-4461-be38-f30f5ebbfad0?expand={expand} request attacker stores into database vulnerable replyUrls value(it is OAuth redirect_uri).

2. To execute XSS user should navigate to OAuth authorization URL with response_mode=form_post and wrong response_type value: https://login.microsoftonline.com/{ATTACKER_ORGANIZATION}/oauth2/authorize?client_id={ATTACKER_CLIENT_ID}&response_type=code1&response_mode=form_post

Medium quality: add repro steps

Steps To Reproduce:

1. Store vulnerable payload into database:
    1. Login to https://portal.azure.com as attacker and navigate to Azure Active Directory-> App Registrations and Add new application.
    2. For application created specify Reply Urls setting as valid https URL like https://newsite.com.
    3. Now setup proxy tool like Burp Suite to intercept browser requests.
    4. Click Save button to store Reply Urls from step 2 and intercept that request in proxy.
    5. In proxy tool replace correct Reply Urls value with vulnerable payload like javascript://newsite12.com/?%0Aalert('XSS%20at%20'%2Bdocument.domain)
    6. Forward request. Now payload should be stored.
2. Run XSS:
    1. Now in another browser log in to another login.microsoftonline.com organization.
    2. Navigate to https://login.microsoftonline.com/{ATTACKER_ORGANIZATION}/oauth2/authorize?client_id={ATTACKER_CLIENT_ID}&response_type=code1&response_mode=form_post -- in that URL replace {ATTACKER_ORGANIZATION} with attacker's organization name, -- in that URL replace {ATTACKER_CLIENT_ID} with attacker's client_id(Application ID) set up in step 1
3. Pay attention XSS alert is run at login.microsoftonline.com.

High quality: include analysis and recommendation

Analysis:

The root cause is missing encoding of untrusted replyURL at login.microsoftonline.com in the following code:

[CODE SNIPPET] - Redacted

Since registered application can be consumer by other Identity services like login.live.com, I tried to render this issue on that service, but failed because of following check:

[CODE SNIPPET] – Redacted

Fix Recommendation:

Properly encode replyURL at login.microsoftonline.com. Make sure to follow best practices for encoding untrusted data as stated at https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.md.

As defense in depth, also see if during ingestion at https://main.iam.ad.ext.azure.com/api/RegisteredApplications, restriction on characters can be applied, that way none of the consumer will be impacted.

Additionally, think of strengthening the service by adding mitigations like CSPs, that way even if there is a XSS, it become harder to exploit.

STRIDE + Quality + Severity = 

Cloud Bounty Program Award Structure

https://www.microsoft.com/msrc/bounty-microsoft-cloud

Impact	Quality	Severity = critical	Severity = important	Severity = medium, low
Remote code execution	High	$20,000	$15,000	$0
	Medium	$15,000	$10,000	
	Low	$10,000	$5,000	
Elevation of privilege	High	$8,000	$5,000	
	Medium	$4,000	$2,000	
	Low	$3,000	$1,000	
Information disclosure	High	$8,000	$5,000	
	Medium	$4,000	$2,000	
	Low	$3,000	$1,000	
Spoofing	High	N/A	$3,000	
	Medium		$1,200	
	Low		$500	
Tampering	High	N/A	$3,000	
	Medium		$1,200	
	Low		$500	
Denial of service	High/low	Out of scope		

Additional tips

Lay out your assumptions

Include your **environment setup details** to avoid reproduction problems and allow our engineering teams to start working on a solution faster.

Think from the attacker’s perspective

To understand severity, put yourself in the attacker’s shoes. What would they gain from exploiting the vulnerability? Thinking through an **attack scenario** may allow you to uncover additional bugs, definer higher-impact scenarios, and unlock larger bounty awards.

We’re working to make it easier to succeed

Program policy updates provide higher awards faster

Increased award levels & scope

- Top awards increased from $15K to $50K for Windows and from $15K to $20K for Cloud
- New scope added for Azure
- More scope to come in 2019!

Award on repro

- In Cloud, Windows, and DevOps bounties, we now award on reproduction (a matter of weeks) rather than fix (a matter of months).
- Finders are still required to withhold public disclosure until the fix is confirmed.

New duplicate policy

- If you’re the first researcher to report a vulnerability that we know about internally but haven’t yet fixed, we still grant full bounty.

Additional resources 

Microsoft Bounty
https://www.microsoft.com/en-us/msrc/bounty?rtc=1

Coordinated Vulnerability Disclosure (CVD)
https://www.microsoft.com/en-us/msrc/cvd

First Steps in Hyper-V research (up to $250,000 bounty award)
https://blogs.technet.microsoft.com/srd/2018/12/10/first-steps-in-hyper-v-research/

STRIDE Model
https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-threats#stride-model

Recent Presentations: Trends in the software security vulnerability mitigation landscape
https://github.com/Microsoft/MSRC-Security-Research/blob/master/presentations/2019_02_BlueHatIL/2019_01%20-%20BlueHatIL%20-%20Trends%2C%20challenge%2C%20and%20shifts%20in%20software%20vulnerability%20mitigation.pdf

Share your feedback on your MSRC experience
msrclistens@microsoft.com.

Conclusion

Focus on high-impact, in scope targets.

Read the bounty brief

High-quality reports earn higher bounty rewards.

1. Repro steps
2. Attack scenarios
3. Root cause analysis

Bounty Program scope will continue to change and grow.

Microsoft

Thank you!

Jarek Stanley
Microsoft Security Response Center

@JarekMSFT
@msftsecresponse
https://www.microsoft.com/en-us/msrc/bounty