Security Reward & Recognition Program

Agenda

- Why?
- Scope
- HowTo
- Rewards
- FAQ

Why

- Different teams
  - Mobile Phones
  - Smart Devices
  - Developer Experience
  - HERE
  - Marketing

=> **Many different WEB sites & services**

Security Teams

- NIRT - IT
- SPC Security Engineering - online services/messaging/HERE
- DX - Store/Publish

Scope

-- In **ALL** countries:

- Mobile APPS (WP8, S40) /* NOKIA/HERE branded only */
- OS Vulns (S40)
- Firmware
- WEB Services
  - Music
  - Nokia Account
  - Store
  - HERE (all geo-location services)
  - etc…
- Client's software
  - NOKIA Music Player
  - NOKIA PC Suite (drivers included)
- Marketing sites and etc…

NOT-IN-Scope

-- In **ALL** countries:

- Dealers (even official)
- Enterprise-corporate systems
- Non-NOKIA services

Report

- **Technical Description**
  - we want to know what you can do, and how you can use it
  - we want to know an **exploitation vector**
- **PoC**
  - we want steps to reproduce your issue
    - Script code
    - URL (SQLi - with getting RDBMS version, XSS - with alert)
    - Packet sample (pcap)
    - etc

Report

- **Please, do not send to us**
  - links to external resources
  - attachments: PDF, DOC, DOCX, EXE, …
    - Allowed: .jpeg, .png, .pcap
  - non exploitable bugs /* self XSS */
  - bugs without evidences
  - bug based on blog articles of someone…
  - risks based on OWASP/CVSS2/One guy told me…

Ethical hackers

#NoMoreFreeBugs

vs.

Responsible Disclosure

Ethical hackers

Why I want to “kill” this bug?

- It was easy to find, so no big deal for me
- I do not expect money, I did it just for fun
- I found it accidently, I do not need this bug

- I WANT TO HELP!

-- *We respect you guys for this, THANK YOU!* --

Ethical hackers

- I want a REWARD!
- Where is my REWARD?
- Facebook has paid me for the same bug XXXX$, so reward me plz. as soon as possible!

- Sure, if we found this as good finding you'll get your reward…

--*Ethical or not?*

Reward & Recognition

- **NOKIA** Hall of Fame
  - For all valid bugs
- **NOKIA** Device
  - **Lumia 820** -> for interesting and dangerous bugs
  - **Lumia 920** -> for super vulnerabilities, that make us cry
- **NOKIA** branded gifts
  - T-Shirt
  - Accessories
  - etc

Reward & Recognition

- Internal committee
  - From different teams, depends from service where bug was found

TEAMS:

NIRT	- Nokia IT
Security Engineering Team	- HERE Platform
Developer Experience	- Developer services
Service teams	- Business owners

Reward & Recognition

- **Dangerous**
  - what can you do? /*open redirect */
  - what can you get? /* open redirect with code*/

- **Interesting**
  - new technique
  - non standard approach /* smart SSRF+authBypass */

We like smart and non-pattern things.

State-of-Art still in price

FAQ

Why you do not reward me for this XSS?

- Our most common recognition is Hall Of Fame

So for XSS it is only one that I can get?

- If your XSS is real threat (stored XSS, that makes possible global ‘infection’ for all users), so maybe not… it’s depends from real vector and threats.
- If internal committee will be surprised (WAF/XSS filter bypass, non-classical case), so maybe not…
- If you did good work with code coverage, then maybe not…

FAQ

Why you do not answer me?

- Please, wait 3-4 days, after yours first e-mail, then you can re-ping us back
- Try to send all your findings in one e-mail, it can help us to work with you

FAQ

Why do not you give me 5.000.000$ for OWASP top 10 bug?

- We respect OWASP, but we calculate our own risk value based on service priority and vulnerability impact.

FAQ

Why do not you give me money, but phones?

- We work with people, community. We want to be friends, and give presents. It’s much better than money ;)
- We spread our brand
- If you all about money, of course you can sell a kidney

Thank you!

Russian community

- **Evgeny Ermakov (Positive Technologies)**
  - From NIRT
- **Sergey Scherbel & Co. (Positive Technologies)** x2
  - From NIRT & SPC
- **Vladimir Vorontsov (ONSec)**
  - From SPC
- **Dmitry Chastuhin (ERPScan)**
  - From NIRT

Q?

Send your bugs and questions to:

security-alert@nokia.com