APNIC’s Vulnerability Reporting Program

Insights from creation to first year of operations

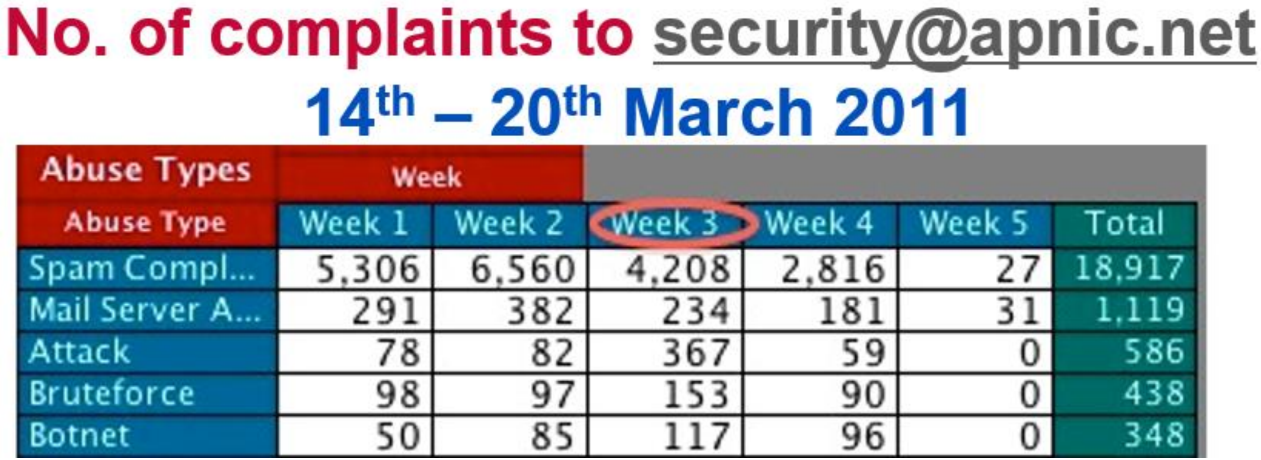
18/02/2022 | Jamie Gillespie

About APNIC

- APNIC is the Regional Internet Registry (RIR) for the 56 economies that makes up the Asia Pacific region
  - Distributes and manages IP address
  - Not-for-profit, purposefully open and transparent
  - Approx 110 staff, mostly in Brisbane Australia
  - Multiple data centres in Australia and internationally
  - IaaS hosting on AWS and GCP, multiple SaaS applications/vendors
  - Not just web sites, but also VPN, SMTP, DNS, FTP, whois, RPKI

In the beginning…

- Very public Helpdesk – helpdesk@apnic.net
  - Used for member enquires, and as a catch-all
- An old security@apnic.net address
  - Used for IRT contacts in whois records



No. of complaints to security@apnic.net

14th – 20th March 2011

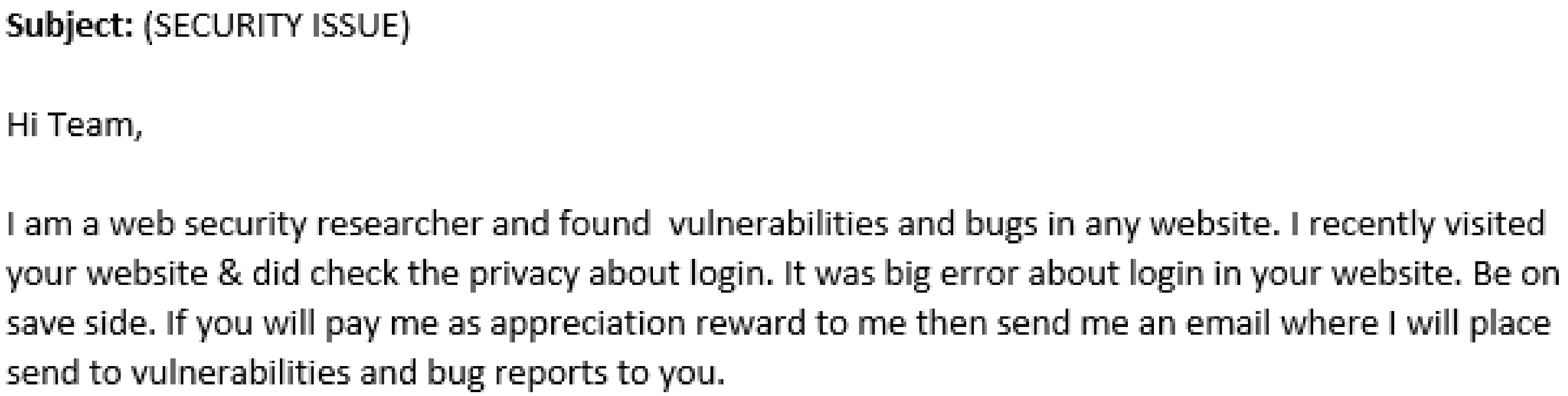
Abuse Types	Week					
Abuse Type	Week 1	Week 2	Week 3	Week 4	Week 5	Total
Spam Compl...	5,306	6,560	4,208	2,816	27	18,917
Mail Server A...	291	382	234	181	31	1,119
Attack	78	82	367	59	0	586
Bruteforce	98	97	153	90	0	438
Botnet	50	85	117	96	0	348

In the beginning…

- APNIC has an internal IT team (or 2)
  - Internal vulnerability scanning
  - External penetration tests
- APNIC also has developers writing new applications
- The APNIC CSIRT was created internally to formalise incident response procedures, and overall information security work

Early vulnerability reports

- Without a proper security point of contact, security researchers would email privacy@ or even hr@ addresses
- Occasional scam email would come in too



Subject: (SECURITY ISSUE)

Hi Team,

I am a web security researcher and found vulnerabilities and bugs in any website. I recently visited your website & did check the privacy about login. It was big error about login in your website. Be on save side. If you will pay me as appreciation reward to me then send me an email where I will place send to vulnerabilities and bug reports to you.

Conception of the VRP

- We should have a point of contact for security researchers
- But we’ll need to advertise it somehow
- We’ll also need to set some rules
- This sounds like a bug bounty program
- Hmmm… but we can’t pay out bounties like the big profit driven companies can
- Would a bug bounty program without the bounties work?

Conception of the VRP

- The APNIC Vulnerability Reporting Program!
  - aka Vulnerability Disclosure Program / VDP
- Reading many other program texts led to a draft VRP
- Draft circulated to IT teams for feedback and improvements
- Used an early template from disclose.io for Safe Harbor
  - disclose.io now have entire VDP generators and templates
- Got the APNIC Legal Team involved to approve the wording

The VRP layout

- Background of APNIC
  - Who we are, what we do
- Introduction of the VRP – “Bug Reporting”
  - “We value the hard work of the security research community, and welcome responsible disclosure of any vulnerabilities in our products and services.”
  - Please use csirt [at] apnic.net
  - Optionally, here is our GPG public key
  - “We aim to reply to all reports within 7 days, and to resolve reported P1-P4 vulnerabilities within 90 day”

The VRP layout

- In Scope
  - *.apnic.net
  - *.apnic.foundation
  - *.isif.asia
  - *.seedalliance.net
  - *.apidt.org

The VRP layout

- Out of Scope
  - 3rd party sites such as Lets Encrypt, Okta, Cloudflare, Zoom, or similar
    - If you inadvertently find an issue with these sites while testing APNIC, we’d like to hear about it. However, we cannot provide permission to test these third parties.
  - Destruction of data
  - DoS/DDoS
  - Social engineering
  - Physical security controls

The VRP layout

- Report Details
  - Repeating the csirt email address
  - “We would appreciate it if your report included the following details”
    - Your contact information, so we can follow up with questions
    - A description of the issue and its nature
    - Detailed steps that allow us to reproduce the issue
    - A brief description of the security impact of the issue
  - “As a not-for-profit, we can’t pay out major bounties, but we really appreciate your help in safeguarding our systems. If we confirm your finding as a vulnerability, we can recognise your contribution in the Thank You section below.”

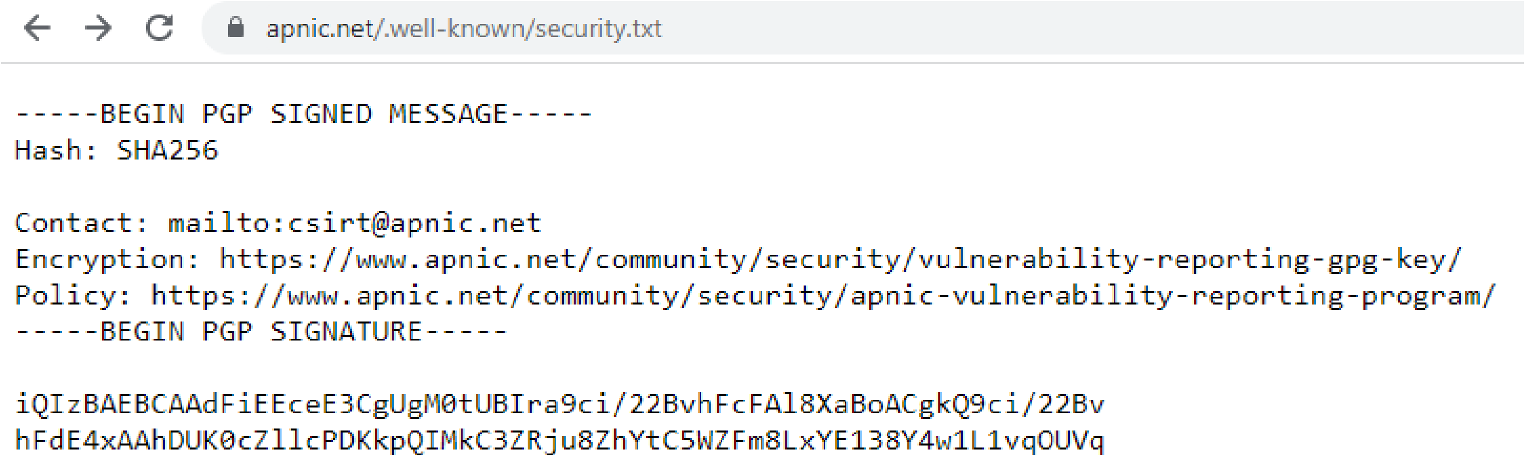
The VRP layout

- Safe Harbor
  - If you conduct vulnerability research that is in scope,
  - and if you report your findings to us in a timely manner

  - We will consider this authorised,
  - and promise not to take legal action against you

Making the VRP accessible

- Generated and published a GPG key for encrypted email
- Creation of a security.txt file with the help of securitytxt.org



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Contact: mailto:csirt@apnic.net
Encryption: https://www.apnic.net/community/security/vulnerability-reporting-gpg-key/
Policy: https://www.apnic.net/community/security/apnic-vulnerability-reporting-program/
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEEceE3CgUgM0tUBIra9ci/22BvhFcFAl8XaBoACgkQ9ci/22Bv
hFdE4xAAhDUK0cZllcPDKkpQIMkC3ZRju8ZhYtC5WZFm8LxYE138Y4w1L1vqOUVq
```

Who is on the receiving end of reports?

- The IT teams will receive reports in the ticketing system
  - csirt@apnic.net already existed, but not publicly used
- The IT teams will manage upgrades of 3rd party software
- What about the code APNIC creates internally?
- THE DEVELOPERS!
  - Oh hey, developers, we didn’t forget about you
  - Can we inject security patching procedures into your development cycle?
  - Can we impose time frames for confirming vulnerabilities, fixing vulnerabilities, testing, and pushing into production?

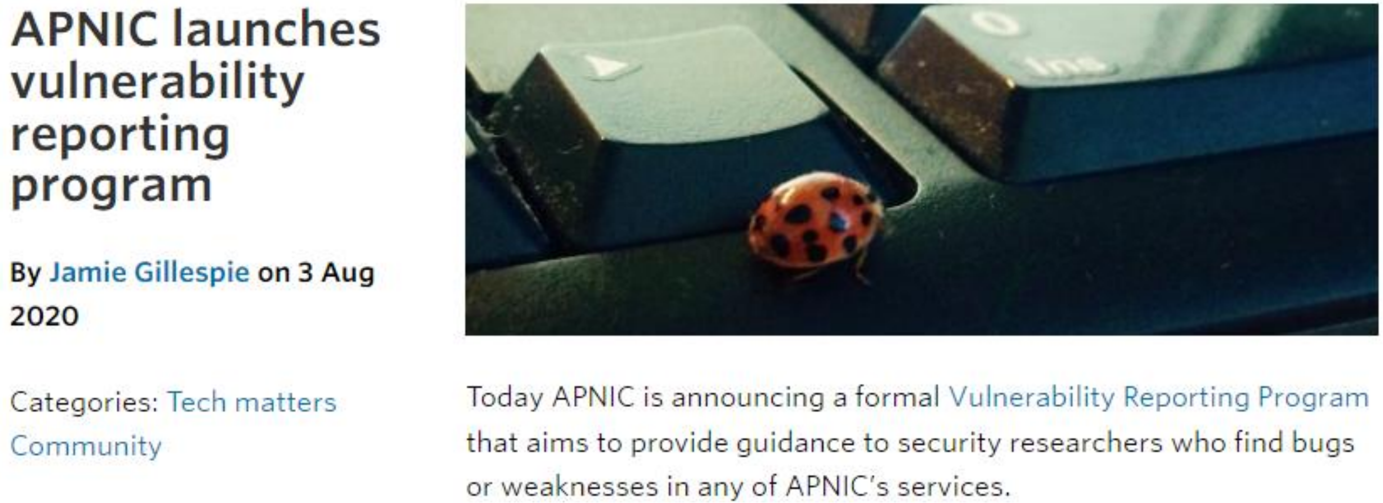
A premature birth

- Just 5 days before the VRP web page is published, a vulnerability report is sent to csirt@apnic.net
  - Stored self-XSS (Cross Site Scripting) in a display name field
- Early test of our vulnerability report handling procedures
- Added a Thank You section to the VRP page, with our early bird security researcher as the first entry.

Thanks Denny!

The (actual) birth of the APNIC VRP!

- VRP web page quietly went live on 28/07/2020
  - https://www.apnic.net/community/security/apnic-vulnerability-reporting-program/
- APNIC Blog post on 03/08/2020
  - https://blog.apnic.net/2020/08/03/apnic-launches-vulnerability-reporting-program/



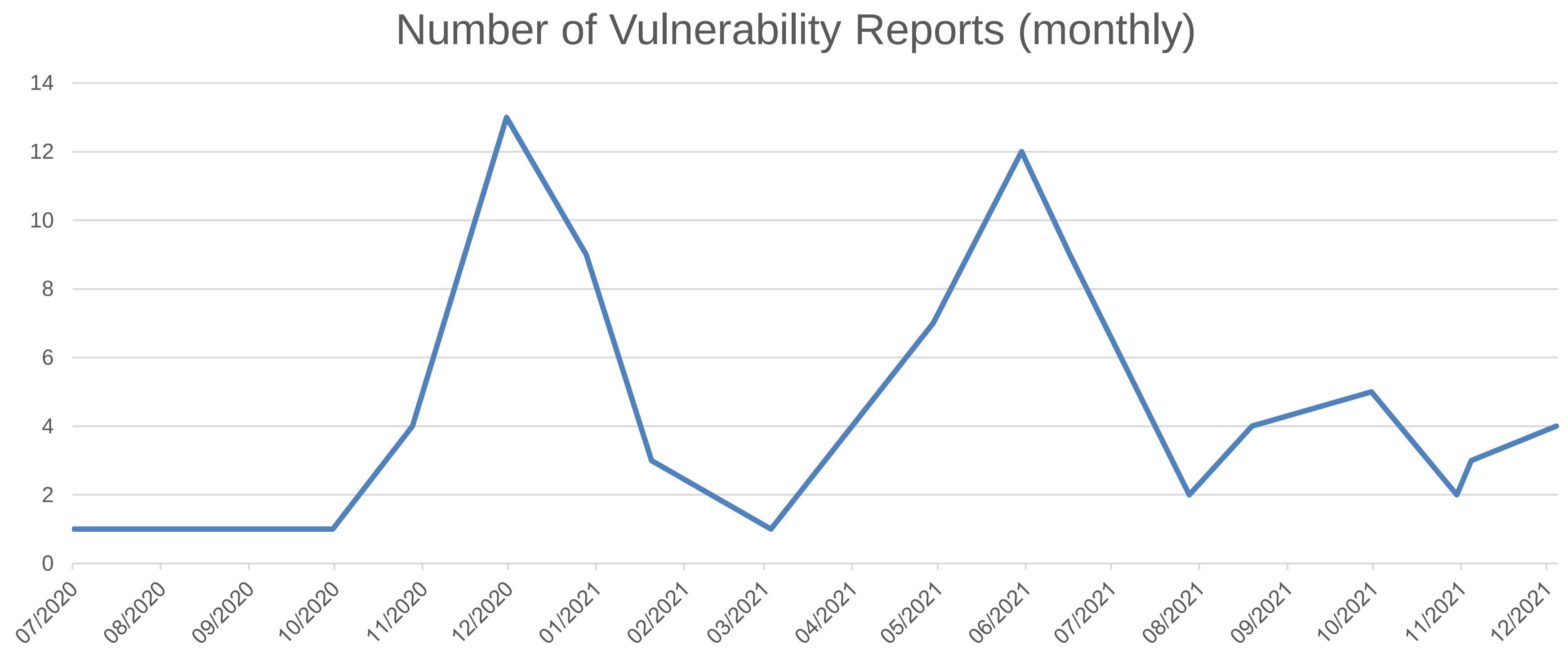
APNIC launches vulnerability reporting program

By Jamie Gillespie on 3 Aug 2020

Categories: Tech matters Community

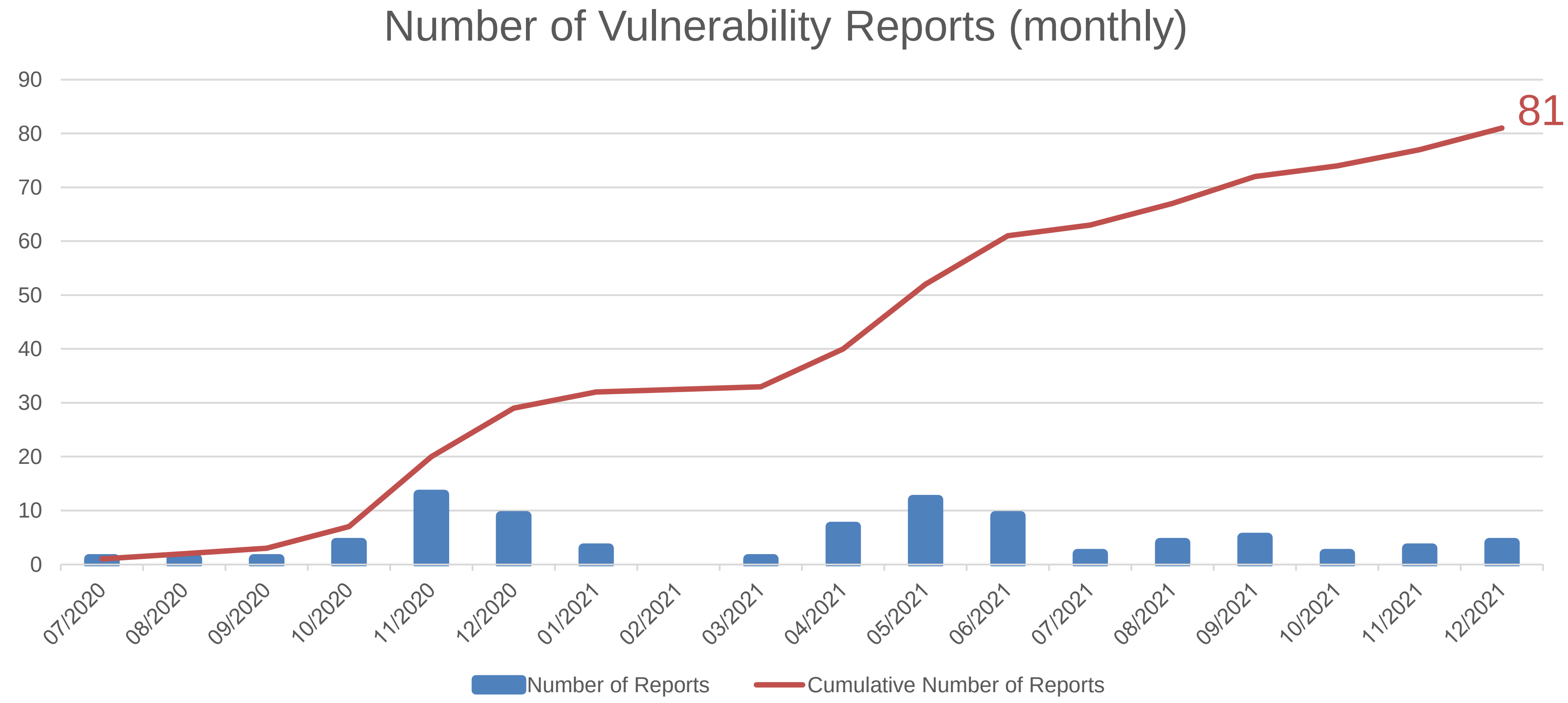
Today APNIC is announcing a formal Vulnerability Reporting Program that aims to provide guidance to security researchers who find bugs or weaknesses in any of APNIC's services.

A slow controlled start



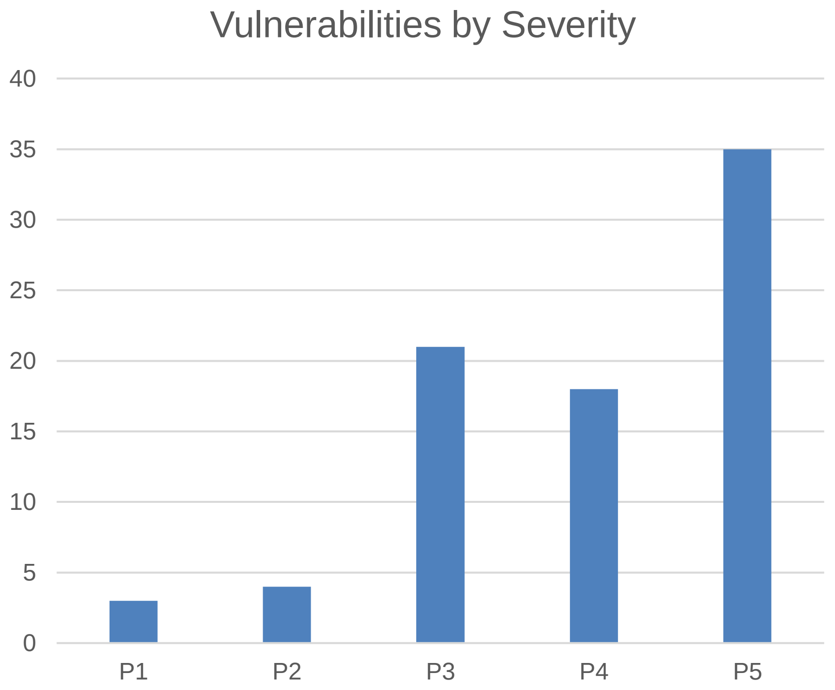
Note: these numbers are based on first reports of unique validated security vulnerabilities

A slow controlled start

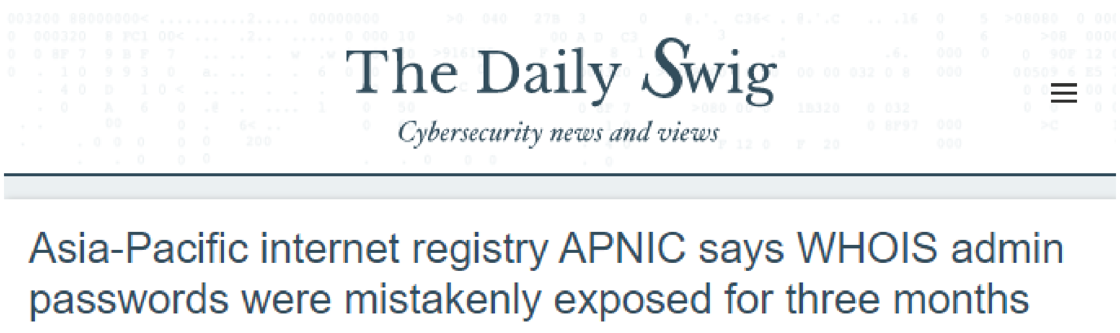


Types and severities of vulnerabilities

- 16 x Information Disclosure
- 10 x Reflected XSS
- 5 x Denial of Service
- 5 x Stored XSS
- 4 x Clickjacking
- 3 x P1 vulnerabilities
  - SQL Injection
  - Sensitive Information Disclosure



P1 Incident that went public



The Daily Swig

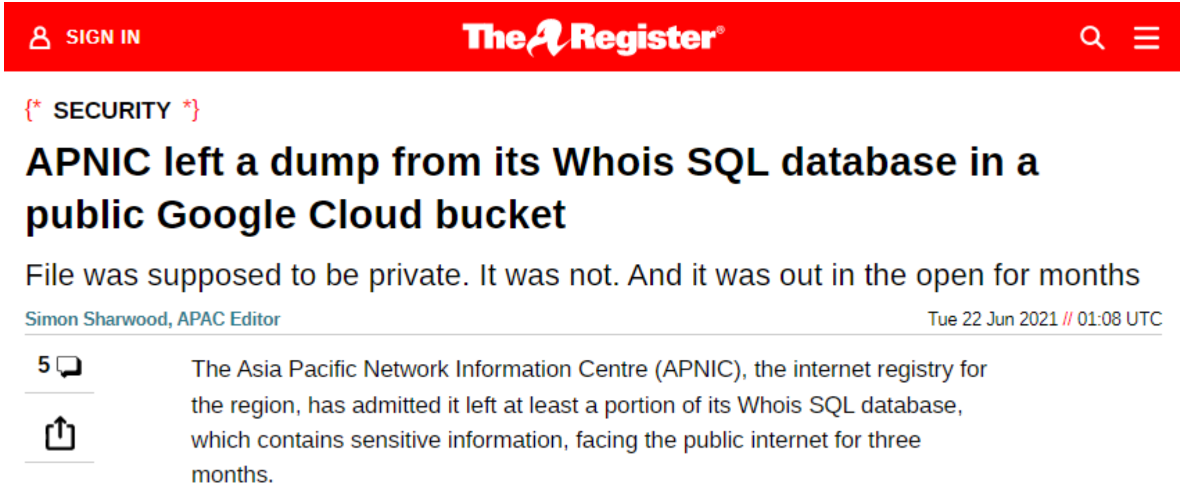
Cybersecurity news and views

Asia-Pacific internet registry APNIC says WHOIS admin passwords were mistakenly exposed for three months

Adam Bannister 22 June 2021 at 14:39 UTC
Updated: 06 July 2021 at 09:29 UTC

Internet Infrastructure | Asia | Data Leak

Internet org downplays threat to integrity of database



{* SECURITY *}

APNIC left a dump from its Whois SQL database in a public Google Cloud bucket

File was supposed to be private. It was not. And it was out in the open for months

Simon Sharwood, APAC Editor

Tue 22 Jun 2021 // 01:08 UTC

5

The Asia Pacific Network Information Centre (APNIC), the internet registry for the region, has admitted it left at least a portion of its Whois SQL database, which contains sensitive information, facing the public internet for three months.

Who reported the vulnerabilities

- 45 security researchers sent in single reports
- 9 security researchers sent in two reports each
- 3 security researchers sent in three reports each
- 1 security researcher sent in four reports
- 1 security researcher sent in five reports
- Most multiple reports came in on the same day
  - Half for the same service, half for different services

Note: these numbers are based on first reports of unique validated security vulnerabilities

Lessons learned

- VRPs / VDPs are useful to complement existing security tools and practices
- Good communication with internal stakeholders is important
  - Before, during, and after launch
- Standard operating procedures and response templates ensure consistent handling of reports and reporters
- Bounties aren’t required to launch a VRP
- Internal reporting to management gets harder with more vulnerability reports and more details being requested

What’s happened since?

- At around the one year mark of operations, APNIC compared the services of vulnerability coordination vendors
- HackerOne was selected to receive, validate, and triage vulnerability reports for APNIC
  - They also provide reporting and privately advertise the vulnerability program to their researchers
- Triaged reports are sent to the APNIC IT team who then route the report to the appropriate product development team

What’s happened since?

- The VRP web page has been updated to include the HackerOne submission form, in preference to csirt@
- The Out of Scope list has been expanded
  - “Working as intended” items such as FTP directory listing
  - Rate limiting issues on non-authenticated endpoints
  - Missing security flags on cookies that don’t relate to authentication
- The “Thank You” list has grown
- APNIC is more secure

QUESTIONS?

Thank You!