Collecting & Disseminating Vulnerability Information

How to gather and distribute security advisories
to your constituency

Klaus Möller
WP8-T1

Webinar, 8th of June 2021

Public

www.geant.org

What we will cover today

- The task
  - How to get the security information from source to destination
- Contents of Security Advisories
  - What should go into an advisory
- Automation standards
  - Machine readability to move work away from admins
- Tools
  - A brief overview of tools for writing and collecting security information

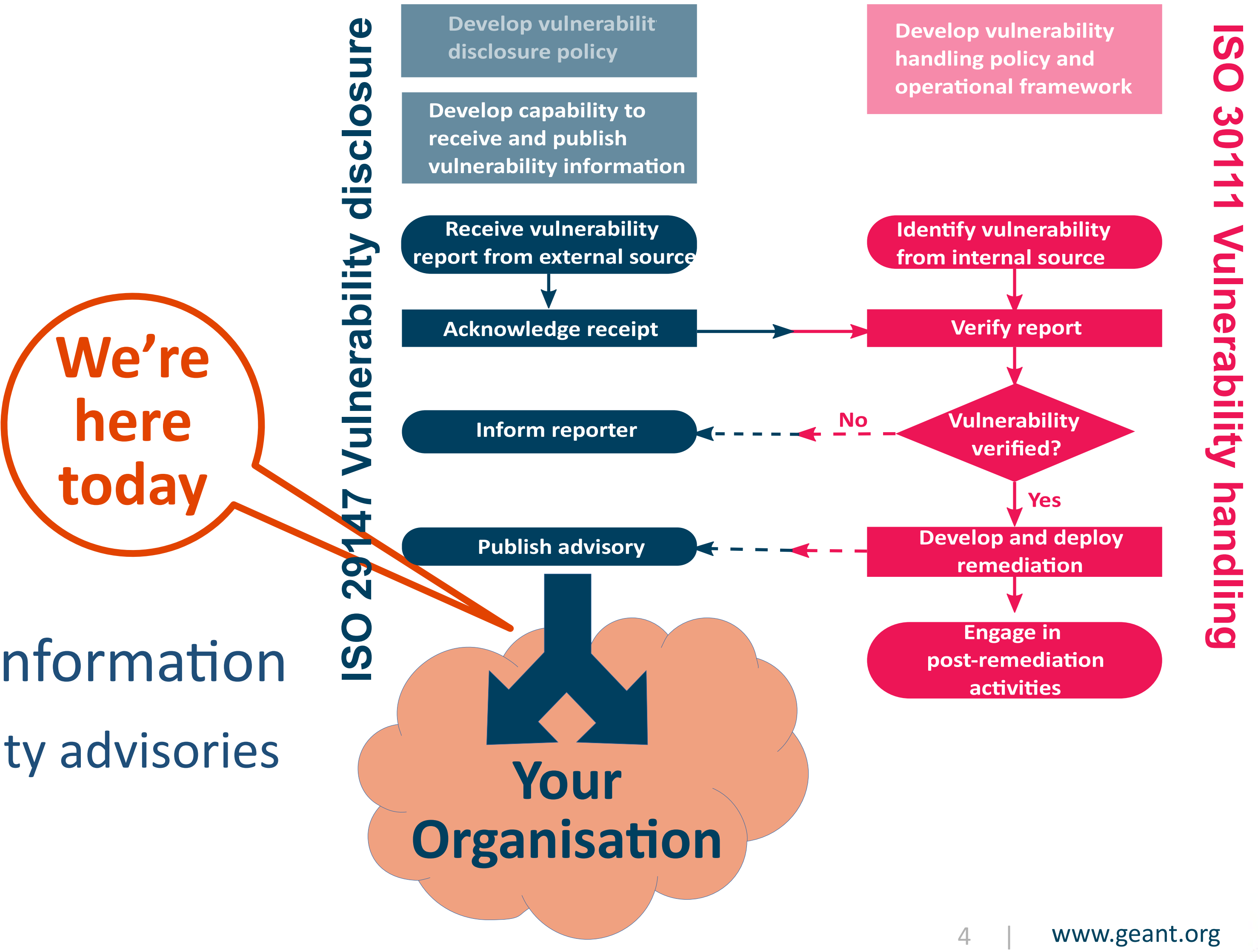
GÉANT
Networks • Services • People

The task

www.geant.org

Collecting & Disseminating Vulnerability Information

- The task:
  - Collecting
  - Filtering
  - Preparing
  - Bundling
  - Distributing
- of vulnerability information
  - Primarily security advisories



We're here today

ISO 29147 Vulnerability disclosure

Develop vulnerabilit disclosure policy

Develop capability to receive and publish vulnerability information

Receive vulnerability report from external source

Acknowledge receipt

Inform reporter

Publish advisory

ISO 30111 Vulnerability handling

Develop vulnerability handling policy and operational framework

Identify vulnerability from internal source

Verify report

Vulnerability verified?

No

Yes

Develop and deploy remediation

Engage in post-remediation activities

Your Organisation

Collecting security advisories

- What are Security advisories?
  - US Committee on National Security Systems (CNSS)*: “Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems.”*
  - Other names: Security Bulletins, Cybersecurity advisories, ...
- At its core: The process of selecting the right advisories for your organization/target group
  - These are not always system/network admins
  - Can be end users, management, etc., i. e. very little technical background
- What do you want them to do with the information in it?

Collecting Information: Quality Criteria

- Relevance
  - Should cover all products used by your organization
  - May require several providers
- Timeliness
  - Advisories should reach you organization/final recipients as soon as possible
  - A certain delay for writing advisories is inevitable, however
- Usability
  - Does the information help getting the job done?
    - What was the job anyway?
- Reliability
  - With regards towards accuracy of information
  - With regards to delivery of the advisories

Collecting Information: Selecting Sources

- Security Mailing Lists: Bugtraq, Full-Disclosure, etc.
- Vendor Announcements: security-alert@..., security-announce@...,
- Security Alert Providers: Flexera, Symmantec, X-Force (IBM), Zero-day Initiative (HP), ...
- CSIRTs: International, National, Organisation-wide, etc.
  - CERT/CC, DFN-CERT, CERT-Renater, CERT-Polska, etc.
    - `https://trusted-introducer.org/directory/index.html`
    - `https://www.first.org/members/teams/`
- Vulnerability databases: CVE, OVAL, exploit DB, etc.
- Your own research: Code audits, vulnerability scans, pentests, etc.
- Other channels: Social media, chats, ...

Filtering

- Goal: Preventing overload by keeping away unneeded information
- Everybody gets only the advisories they need/are interested in
  - Windows admins get Windows advisories only
  - Linux admins get Linux advisories only, etc.
- Optional: De-duplication of redundant information
- At the very least filtering by keywords in E-mail subject lines

Preparing

- Interpret information for local constituency
  - Suited to skill level, common platforms, etc.
  - Help readers, don’t just frighten them!
- CSIRT writes own reports or introductions
  - Can use multiple sources of information
  - E. g. open source, observed activity
- Sometimes translation into local language
- Interpretation takes time
- Getting people to act takes even longer!

Bundling

- Recipients most likely won’t be bothered with too many announcements in short time
- But this may happen
  - Vendor may publish one advisory per vulnerability/per sub-product
    - Think of office suites (text processor, spreadsheet, …)
  - If information flow is not real-time, announcements may pile up
    - Or the vendor publishes only a few times/year
- Advisable to bundle information if this helps the recipients
- Finding suitable criteria is difficult
  - Usually by trial-and-error (and recipients’ feedback)

Distribution

- Pass information from others to own constituency
  - Typically means maintaining a mailing list/web site
- Goal is to publish before widespread attacks
  - Targeted advice should be implemented sooner
- Decide which advisories are archived, and how
  - Revision histories are helpful

Distribution: Securing the channel

- Advisories should be cryptographically signed if possible
  - E. g. PGP or S/MIME
  - Signing may be tricky, e. g. with web pages
- Do not confuse with TLS/SSL
  - But (transport) encryption may help too
- Encourage checking: fake “advisories” are common
- Advisories should have reference numbers
  - Helps readers and other teams
- Include status, date & time (UTC)

Contents of Security Advisories

www.geant.org

Advisory Contents: Vulnerability Information

- Public name of the problem (i. e. vulnerability)
  - Like HEARTBLEED, POODLE, etc.
  - Other names for the same problem
  - CVE Identifier and other identifiers (Securityfocus Bid No, Bugzilla ID, etc.)
- Description of the vulnerability, i. e. plain text
  - Is this suitable for the target group?
- Severity of the described vulnerability
  - Most often the CVSS score now
  - Is the temporal score given or only the base score?
    - Needed if threat assessment (theoretical, …, present) should be done
  - Access Vector?

Advisory Contents: Vulnerability Information (cont.)

- Platforms affected by the vulnerability
  - List all CPEs, if possible
  - This list will grow over time
  - Remember: outdated software may still be vulnerable, but gets no patch
- Impact of the vulnerability - what happens when it is exploited
  - What is the damage (compromise, DoS, etc.)?
  - What privileges would be gained?
  - What data would be disclosed, modified, …?

Advisory Contents: Remediation Information

- Workarounds
  - Are there workarounds to the problem
  - How can they be applied
  - Do they remediate the problem completely or partially?
- Solution
  - Type of the solution (patch, config change, …)
  - Side effects of the solution, i. e. incompatibilities

Advisory Contents: Remediation Information (cont.)

- Software Updates, i. e. patches
  - For which versions/platforms do updates exist?
  - Versions/platforms where updates will be released in the future
  - Supported versions/platforms that are affected but don’t get updates
  - How to check if the update is required or has already been applied
- Diagnosis information
  - How to detect a vulnerability/compromise
  - Indicators of Attack (IoA)
  - Indicators of Compromise (IoC)
  - Ask your SOC/CSIRT

} Coredump files, log messages, etc.

Advisory Contents: Miscellaneous Information

- URL where the advisory can be found
  - A reference when looking at the updated advisory later
- Revision notes
  - History of changes to the advisory
  - Status of advisory (draft/interim/final/update)
- Credits
  - To the original finders of the vulnerability
- Contact
  - For feedback to the advisory writers/publishers
- Digital signature information
  - I.e. the certificate of the public key the advisory has been signed with

Automation standards

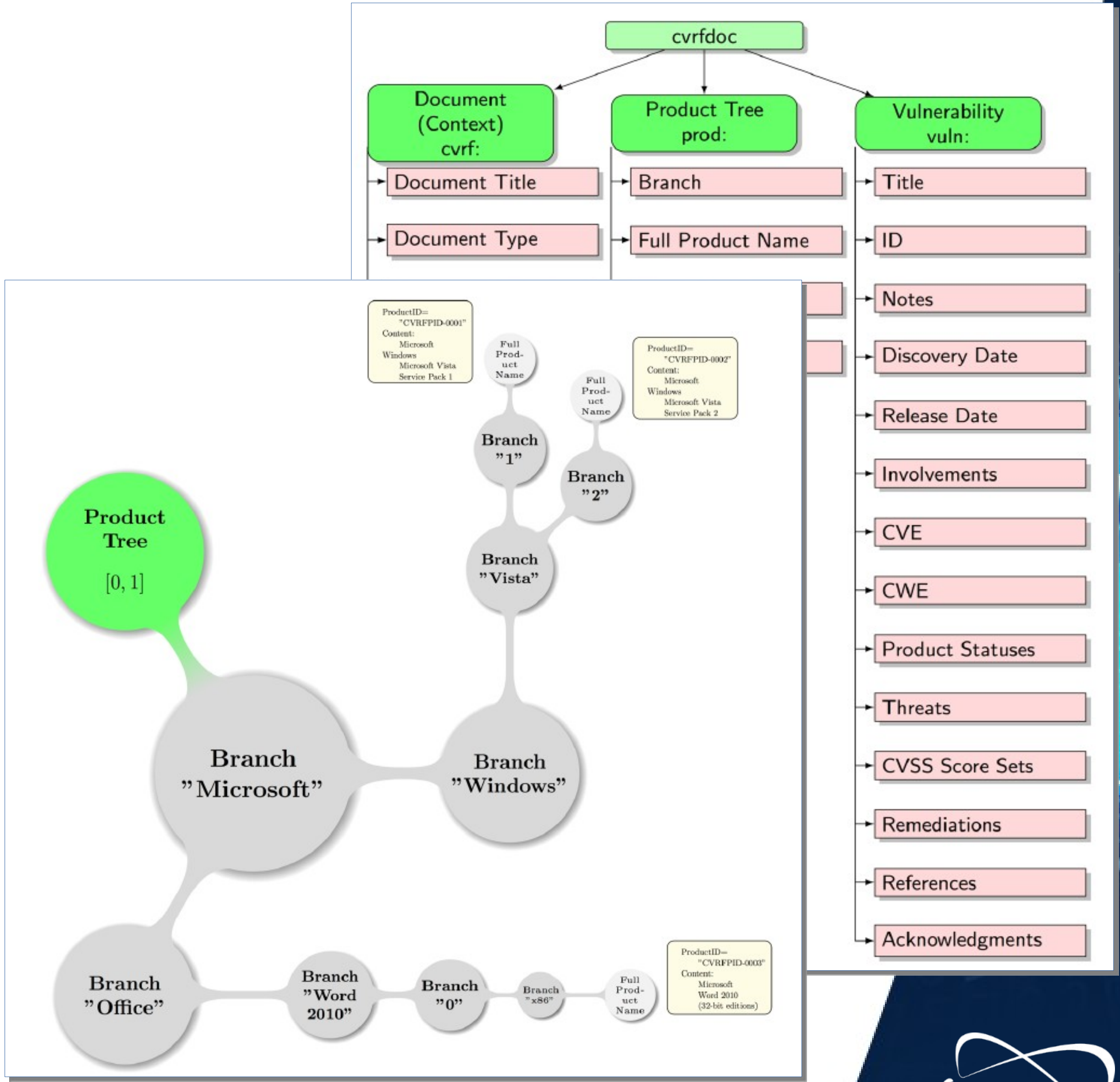
www.geant.org

Machine readable formats

- Automation is the key to efficiency
  - Information has to be machine readable, i. e. have a standardized structure
  - Free text formats change to often, too much work to keep parsers up to date
  - Most utility with filtering, searching, and aggregating information
- Common Vulnerability Reporting Format (CVRF)
  - Version 1.2 from 201x, not backward compatible with version 1.1
  - XML-based
- Common Security Advisory Format (CSAF)
  - Version 2.0 - in continuation of CVRF version numbering
  - JSON-based

CSAF/CVRF Data Model

- Document metadata
  - Title, revision history, etc.
- Affected products
  - Organized by branches and/or product families
- Vulnerability
  - Utilizes CVE, CVSS, CWE, etc.
- Support
  - Most vendors use their own format
  - or CVRF v1.1/ v1.2
  - Very little support for CSAF 2.0 yet



Source: CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2

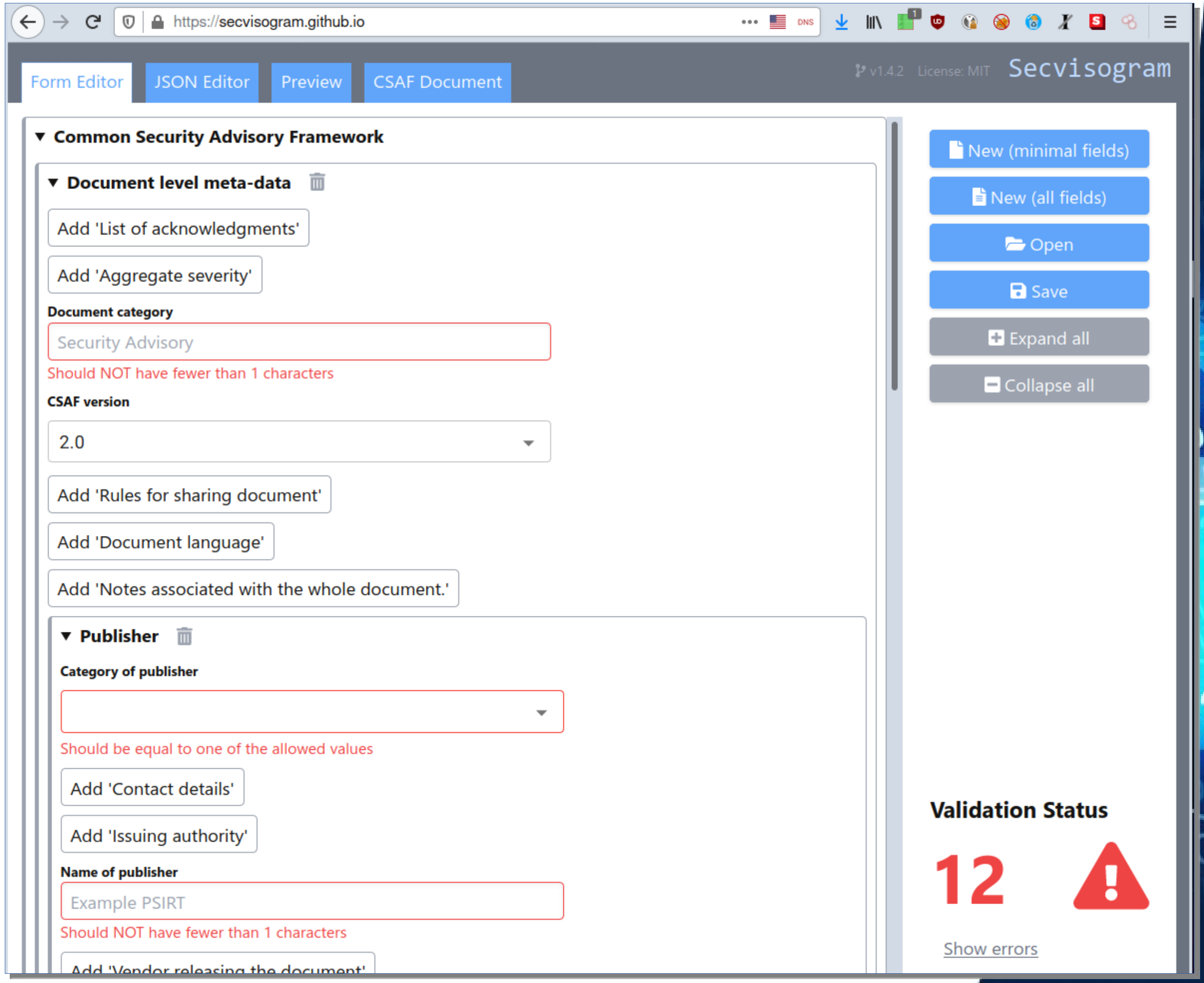
GÉANT
Networks • Services • People

Tools

www.geant.org

CSAF Tool: Secvisogram

- Developed by German BSI (Federal Office for Information Security)
- Inspired by Vulnogram (older advisory writing tool)
- Node.js application
  - Client only (no auth. req.)
  - ACE JSON editor
  - Preview templates via `{{ mustache }}` library



https://secvisogram.github.io

Common Security Advisory Framework

Document level meta-data

Document category: Security Advisory

Should NOT have fewer than 1 characters

CSAF version: 2.0

Publisher

Category of publisher:

Should be equal to one of the allowed values

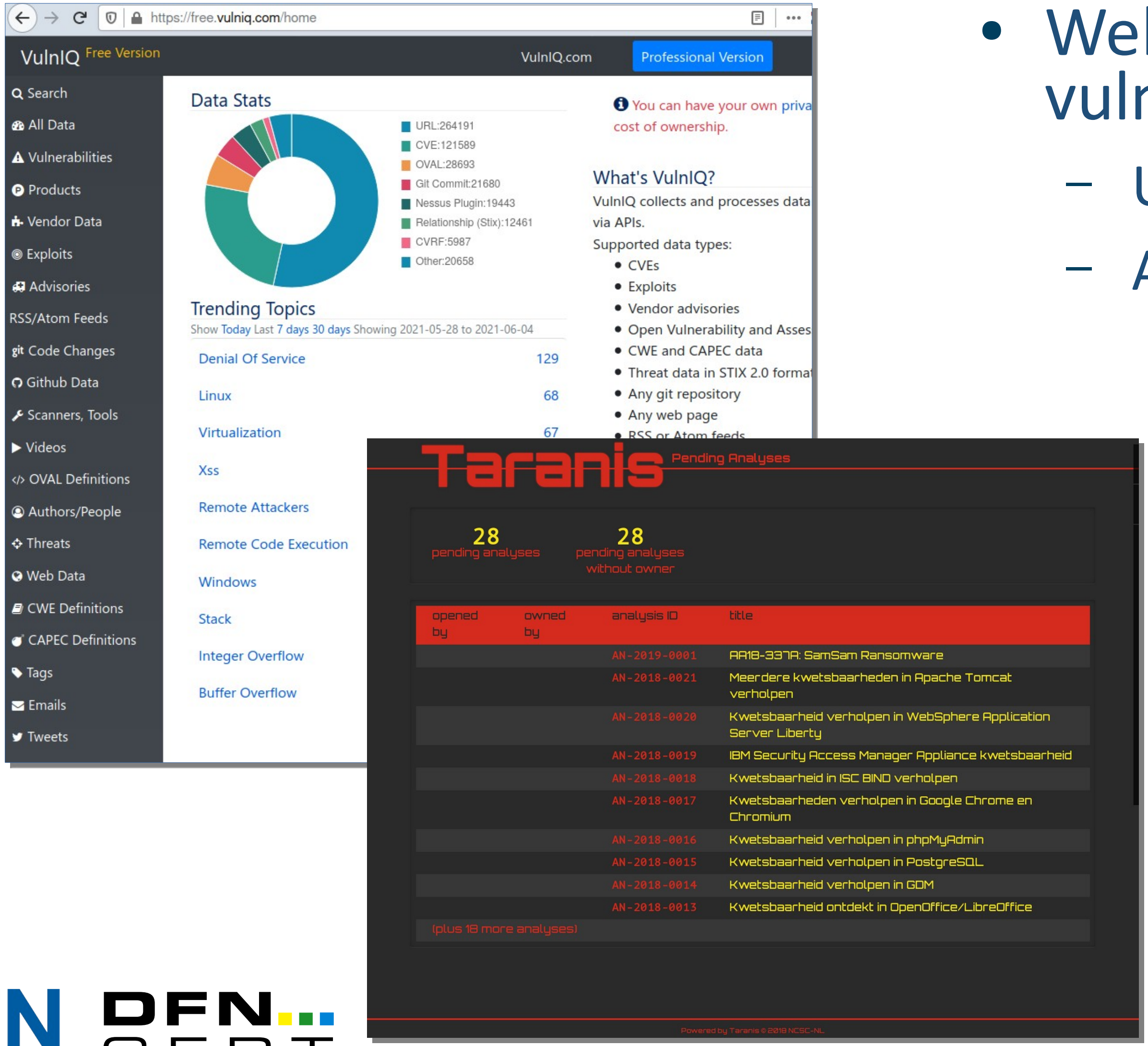
Name of publisher: Example PSIRT

Should NOT have fewer than 1 characters

Validation Status

12

Data Collection Tools/Sites



Data Stats

You can have your own priva
cost of ownership.

What's VulnIQ?

VulnIQ collects and processes data
via APIs.

Supported data types:

- CVEs
- Exploits
- Vendor advisories
- Open Vulnerability and Asses
- CWE and CAPEC data
- Threat data in STIX 2.0 format
- Any git repository
- Any web page
- RSS or Atom feeds

Trending Topics

Show Today Last 7 days 30 days Showing 2021-05-28 to 2021-06-04

Denial Of Service	129
Linux	68
Virtualization	67
Xss	
Remote Attackers	
Remote Code Execution	
Windows	
Stack	
Integer Overflow	
Buffer Overflow	

Taranis Pending Analyses

28 pending analyses

28 pending analyses without owner

opened by	owned by	analysis ID	title
		AN-2019-0001	AA18-337A: SamSam Ransomware
		AN-2018-0021	Meerdere kwetsbaarheden in Apache Tomcat verholpen
		AN-2018-0020	Kwetsbaarheid verholpen in WebSphere Application Server Liberty
		AN-2018-0019	IBM Security Access Manager Appliance kwetsbaarheid
		AN-2018-0018	Kwetsbaarheid in ISC BIND verholpen
		AN-2018-0017	Kwetsbaarheden verholpen in Google Chrome en Chromium
		AN-2018-0016	Kwetsbaarheid verholpen in phpMyAdmin
		AN-2018-0015	Kwetsbaarheid verholpen in PostgreSQL
		AN-2018-0014	Kwetsbaarheid verholpen in GDM
		AN-2018-0013	Kwetsbaarheid ontdekt in OpenOffice/LibreOffice
(plus 18 more analyses)			

Powered by Taranis © 2018 NCSC-NL

- Websites to aggregate vulnerability information
  - Usually closed source
  - API access through paid subscription

- Free engine: Taranis
  - From Dutch National Cyber Security Center (NCSC)
  - Perl, lots of dependencies

What have you learned?

- Collecting and distributing advisories is mostly straightforward, but requires work
- Machine readable information required to automate tasks
  - I. e. CVRF/CSAF
- Some tools already exist but do not cover all the work
- Some other tools will be there already
  - E. g. mailing lists, web CMS, TTS, etc.
- Deliberately not covered: How to write advisories
  - This is the job of (C|P)SIRTs & pentesters - not our target group today
  - And there are good courses and documents already

GÉANT
Networks • Services • People

Thank you

Any questions?

Next Module: ***Patch Management***, 10th of June 2021

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

References

- Definition of Security Advisory, Committee on National Security Systems (CNSS) Glossary: April 2015, https://www.cnss.gov/CNSS/openDoc.cfm?D+KvJjHbdxIaV9BJJ4stHw==
- ENISA Training: “Writing Security Advisories”, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/writing-security-advisories-handbook
- How to Build a CIRT based on Open source tools, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_Cyberdrill_18/Presentations/5-Services.pdf
- CVRF: https://www.icasi.org/cvrf/
- CSAF: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf

Databases, Aggregators & Tools

- CVE List: `https://cve.mitre.org/cve/`
- ITSecDB: `https://www.itsecdb.com/oval/`
- OpenCVE: `https://www.opencve.io/`
- CVEDetails: `https://www.cvedetails.com/`
- VulnIQ: `https://free.vulniq.com/advisory/home`
- CIRCL: `https://cve.circl.lu/`
- Secvisogram CSAF 2.0 editor: `https://secvisogram.github.io/`
- Vulnogram: `https://github.com/Vulnogram/Vulnogram`
- NCSC-NL Taranis3 `https://github.com/NCSC-NL/taranis3`