Security Conference 2022

Coordinated Vulnerability Disclosure: the Perspective of a Telco Vendor

Security in our DNA, Trust Through our Transparency

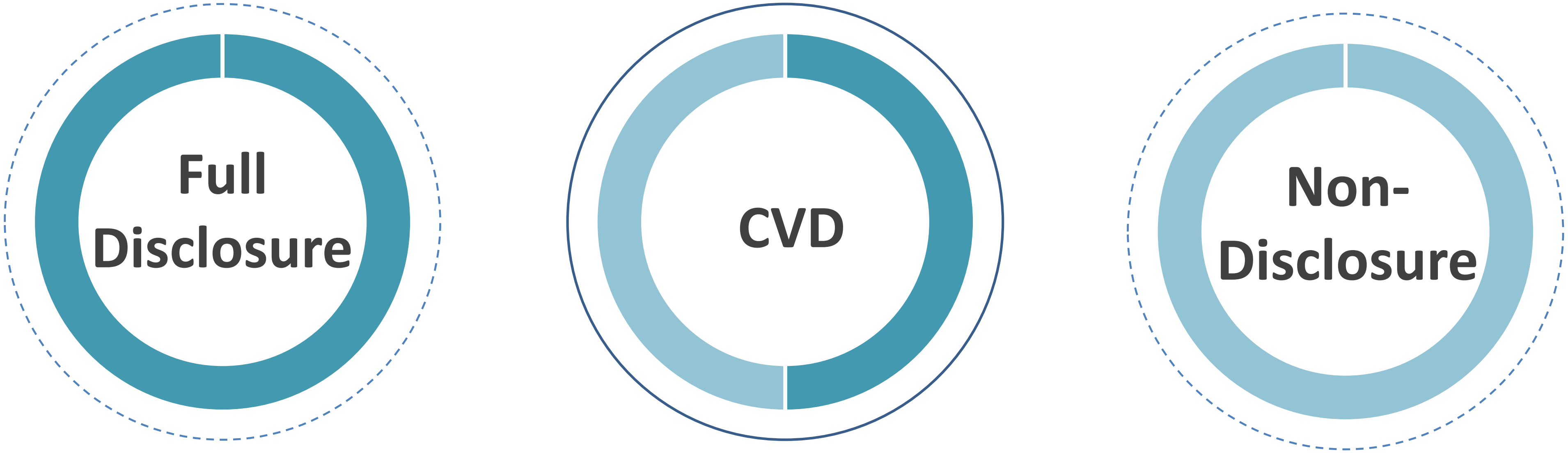
Luca Bongiorni

05/Oct/2022

Contents

- Disclosure Status
- ZTE's Approach on Vulnerability Response
- Case Study
- Conclusion

Vulnerability Disclosure: Global Overview



Full Disclosure

Making a vulnerability fully public

CVD

Coordinated Vulnerability Disclosure

Non-Disclosure

Selling or using a vulnerability yourself

**Source: Coordinated Vulnerability Disclosure: The Guideline — NCSC*

Telco's Vulnerability Disclosure Status

Most of Telco products are not accessible by a wider audience

Require mutual agreement on O&M between MNO & vendor

3rd party component management

Harsh time pressure for the end-to-end response process

Contents

- Disclosure Status
- ZTE's Approach on Vulnerability Response
- Case Study
- Conclusion

Receive Verify Disclosure Fix

Where to find ZTE's VDP: ZTE hackerone YES WE HACK

Coordination

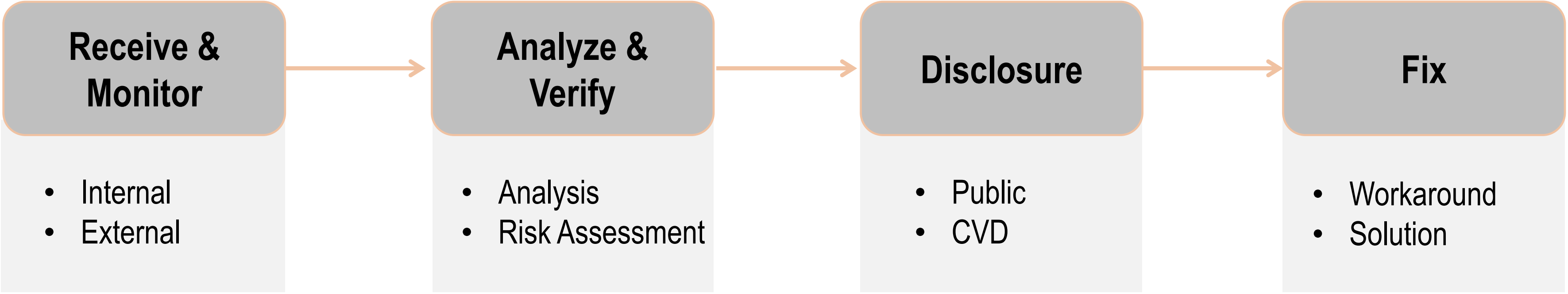
FIRST CERT GSMA CVE CNCERT/CC CNVD CNNVD 国家信息安全漏洞库

Where to find ZTE's VDP: ZTE hackerone YES WE HACK

Coordination

FIRST CERT GSMA CVE CNCERT/CC CNVD CNNVD 国家信息安全漏洞库

ZTE's Approach on Vulnerability Response



Receive & Monitor

- Internal
- External

Analyze & Verify

- Analysis
- Risk Assessment

Disclosure

- Public
- CVD

Fix

- Workaround
- Solution

How to Find Vulnerabilities

ZTE

Internal

Source code check

FORTIFY
RogueWave Klocwork
coverity A Synopsys Company

3rd party component

BLACKDUCK by Synopsys
CYBELLUM

Penetration testing

BURPSUITE PROFESSIONAL
KALI LINUX
Nmap
sqlmap
HYDRA
BeEF
netcat
RAPID7 metasploit

Web security testing

MICRO FOCUS WebInspect
HCL AppScan
acunetix

Fuzzing test

SYNOPSYS Defensics
PEACH FUZZER

System scanning

tenable Nessus
NSFOCUS

External

Reported by customers

Reported by components suppliers

/CERT/

Reported by white hat/CERT/other 3rd party

Most Important 2 steps for Verifying Vulnerabilities

Vulnerability Analysis

- Identify the vulnerability
- Reproduce the vulnerability and verify severity
- Locate the root cause

Risk Assessment

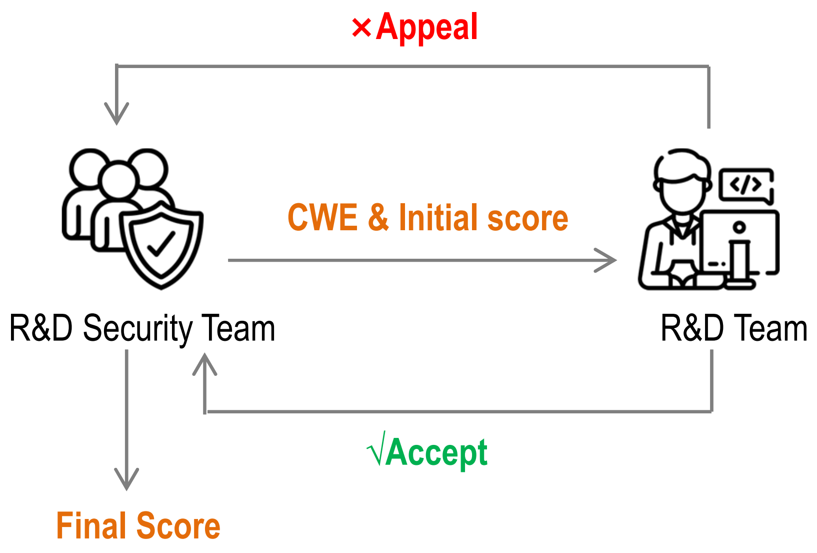
- Prioritize the vulnerabilities
- Scope affected versions and products
- Convey the possible damage that the exploit might cause

Severity Classification of Vulnerability

Severity of Known Vulnerability

Level	Base Score Range (CVSS v3.0 Rating)
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9

Severity of Newly Discovered Vulnerabilities



×Appeal

CWE & Initial score

R&D Security Team

R&D Team

√Accept

Final Score

Disclosure

Coordinated Vulnerability Disclosure：

- **Customer-oriented:** ***Abide by the Law and Service-Level Agreement Always Come First***
  - **Critical/High:** ZTE's E&S teams communicate with customers at the earliest time according to the technical notice released by R&D.
  - **Medium/low/open issues:** ZTE's E&S teams regularly communicate with operators' branch offices to disclose the vulnerabilities and fixing progress.

Public Disclosure:

- Public Security Bulletin: https://support.zte.com.cn/support/news/NewsMain.aspx including the following information:
  - Release date
  - CVE ID
  - Severity
  - Description
  - Affected products and version
  - Mitigation or solutions

**E&S: Engineering and Service, who provides operation & maintenance services.*

Fix: Provide a Workaround and Solution

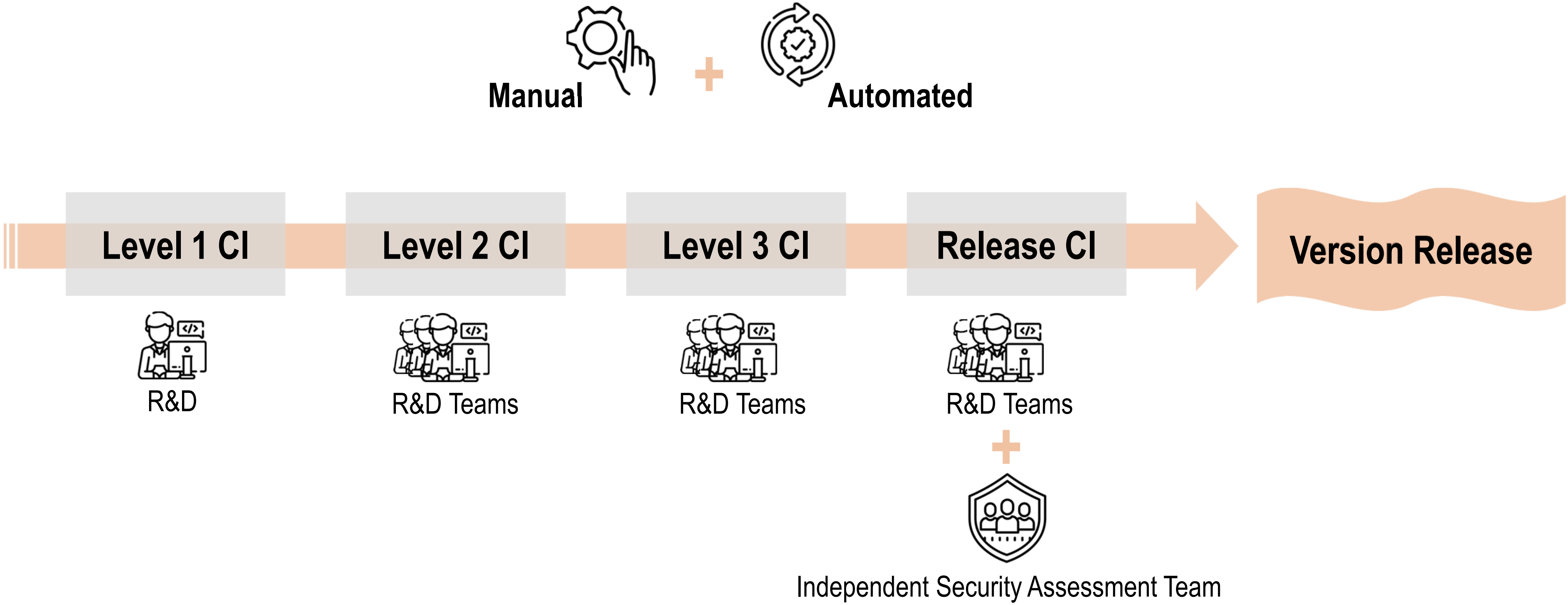
Abide by the Law and Service-Level Agreement Always Come First

ZTE *'s Regulations*

Incident Response Time	
Level	**Mitigation Time**
Critical	*4 Hours*
Major	*24 Hours*
Significant	*2 Days*
Minor	*7 Days*

Vulnerability Handling Time		
Level	**Mitigation Time**	**Formal Solution**
Critical $^{\text{CVSS: 9-10}}$	*7 Days*	*45 Days*
High $^{\text{CVSS: 7-8.9}}$	*7 Days*	*45 Days*
Medium $^{\text{CVSS: 4-6.9}}$	-	*90 Days*
Low $^{\text{CVSS: 0-3.9}}$	-	*Abide by law & SLA*

Solutions are Integrated into New Version Release



** CI: Continuous Integration*

Independent Security Assessment

ZTE Cyber Security Lab

Value Added

A transparency platform for global customers, regulators and other stakeholders to perform independent security assessment of ZTE products, services and processes

Function Verification

Source code review

Document review

Penetration testing

Knowledge transfer

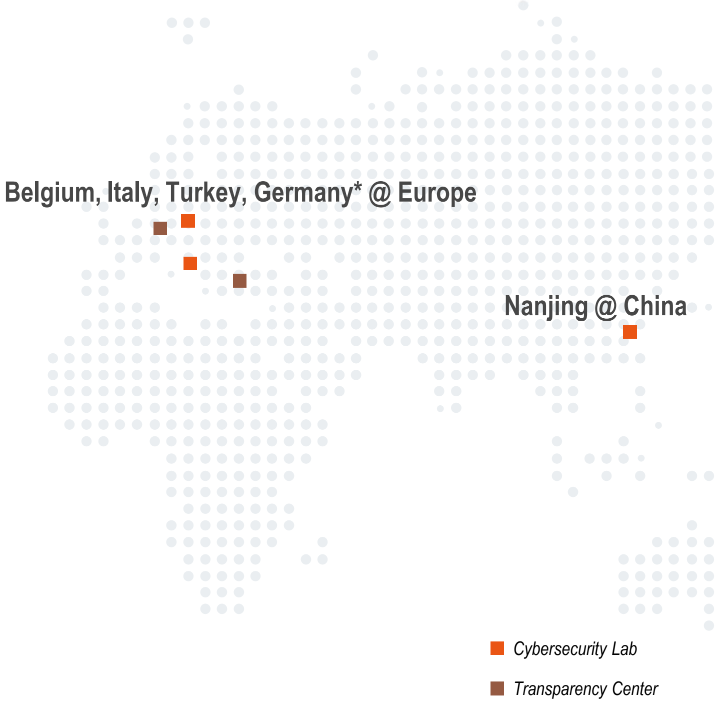
3rd Party Verification

Product security evaluation

Process assessment

Security maturity assessment

Testing supervision



** Cybersecurity Lab of Germany is under construction*

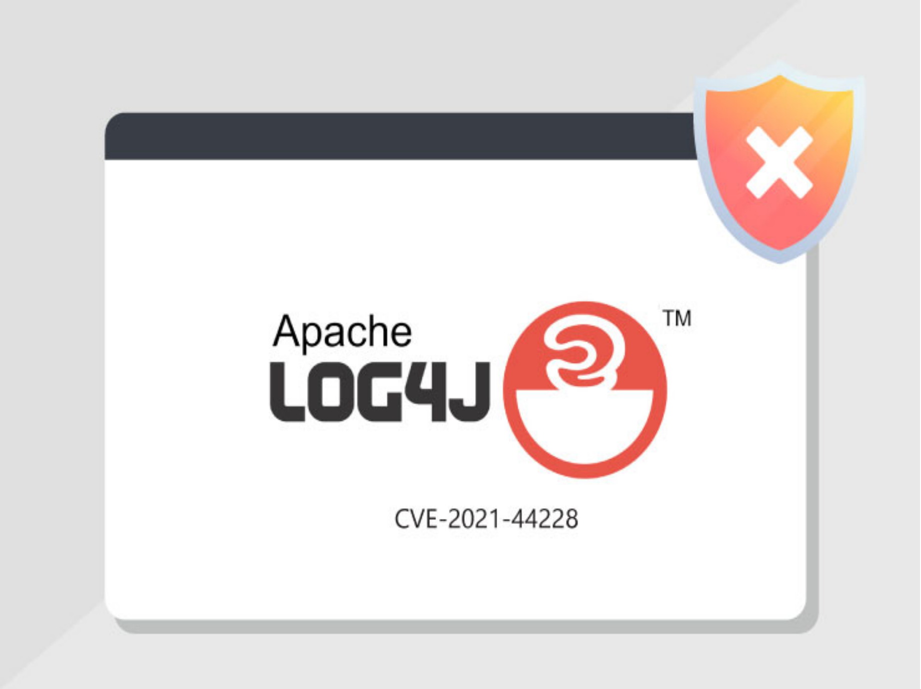
GSMA CVD Panel of Experts (PoE)

- ZTE: two experts in GSMA PoE group, working with Telecom's industry stakeholders
- Enables early notification of vulnerabilities
- Provides time to respond and remediate vulnerabilities before they become public
- Builds trust with security researchers and organisations
- Improves security awareness and readiness

Contents

- Disclosure Status
- ZTE's Approach on Vulnerability Response
- Case Study
- Conclusion

Apache Log4j Vulnerability



Multiple Channels

2022.12.09 PSIRT/customers/suppliers started to report this issue.

Quick Response

- **All product:** Check and analysis;
- **Affected products:** Provide solutions within specified time requirements;

Open and Transparent Disclosure

- **First notice:** Announce affected products on ZTE website;
- **Within 7 days:** R&D provided mitigation and released the notification;
- **Follow-up:** Fully solved issues in newer releases after communicating with customers.

Contents

- Disclosure Status
- ZTE's Approach on Vulnerability Response
- Case Study
- Conclusion

Responsible, Timely, Coordinated and Transparent

ZTE CVD Hackathon 2023

- 1st Cybersecurity CVD Hackathon of this kind!
- Open to Security Researchers, MNOs, Universities and Government Personnel!
- Access to 5G Telco targets!
- Pilot happening in 2023 in Rome!
- For more information contact us:

CybersecurityLabEU@zte.com.cn

Security Conference 2022

Thank You!

Luca Bongiorni

05/Oct/2022