jtsec

BEYOND IT SECURITY

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Patch Management
for
ISO/IEC 15408 / Common Criteria

Javier Tallón, jtsec
Sebastian Fritsch, secuvera
2022 International Conference on the EU Cybersecurity Act 25.05.2022

- Overview
  - Patch problem description
  - ISO/IEC TS 9569: Towards Creating an Extension for Patch Management for ISO/IEC 15408 and ISO/IEC 18045
    - Concept
    - Practical considerations
  - Implications of Patch Management in the EUCC Scheme
    - Patch levels
    - EUCC Next steps
  - Conclusions

secuvera

Patch problem description

- Patch problem description
  - Risk owner requirements
    - demand for certificate of product (TOE): assurance
    - but also for state-of-the-art security
      - security issue handling during product lifecycle
      - delivery of security updates
      - maintenance/support processes

- Patch problem description
  - As consequence risk owner often…
    - …has to accept known vulnerabilities
    - … can install patched but non-certified TOE updates

- Patch problem description
  - Problems of patch re-certification
    - costs and time for patch re-certification
    - only done if mandatory required by regulation
  - Product time to market
    - Continuous delivery
    - Vulnerabilities are made public and patched everyday
    - But re-certification of patches is slow
  - Security vs. Certification → *really ?*

- Patch problem description
  - Chances of this proposal
    - risk owner’s requirements will be addressed
    - regulatory body can request risk owners to install updates to remove existing vulnerabilities
    - modernized our CC toolbox
      - offer fast-track process
      - use assurance from patch management process evaluation
      - …
      - real chance to mandate re-certification (in regulation or contracts)

ISO Project

ISO/IEC TS 9569:
Towards Creating an Extension for Patch Management
for ISO/IEC 15408 and ISO/IEC 18045

- History and future
  - Patch Management is hot topic in ISO SC 27/WG 3
    - Multiple study periods
    - Project was upgraded from TR to TS
    - (new) CC Roadmap discussions already refer to Patch Management Project

      → a lot of support

- Concept
  A. One static + one flexible building blocks
     1. ALC_PAM
        - evaluate Patch Management Process as part of the standard evaluation (certification)
        - ready for augmentation
     2. Patch/Update functionality in TOE scope
        - technical security capabilities for applying patches
        - Package for Patch Management: SPD, objectives and set of SFRs
          - » attached as Annex
          - » written as example
        - finally defined in the ST or PP
  B. Options for Certification Bodies

- New family ALC_PAM
  - ALC_PAM.1 Patch Management Processes
  - key elements:
    - security relevance report (SRR)
      - Developer's self-assessment of security relevance of a planned patch
    - Patch Management Processes (PAM Processes)
      - require Patch Management Documentation (PMD), i.e. policies, processes, procedures and tools related to the patching of the TOE
        - » mandatory procedures during patch release
        - » polices when to re-certify/re-evaluate the TOE
        - » end-of-support consideration of TOE
        - » assessment and confirmation of the application of policies on a regular basis

- Options for Certification Bodies for cherry picking

  - Fast-Track Re-Certification
  - Different types of updates and related re-certification possibilities
  - Support re-use of evaluation results
  - Same-evaluator requirement
  - Re-Evaluation (without Certification)
  - Provide templates to support the analyse impact of changes of a patch
  - Trust by default developers in order to harmonize security and certification
  - Put penalties if developers do not follow the published rules
  - Mandate root cause analysis

- How to apply: practical considerations

  Guide for ST/PP authors:

  - add Extended Component Definition (ALC_PAM.1) to ST/PP
  - add Evaluator Work Unit to ST (or link referenced document)
    - both defined in ISO document
  - write Security Problem Definition (SPD), Objectives (for Patches) and SFRs
    - example is given in ISO document
  - watch out for ST/PP examples which include ALC_PAM.1 in the future

- first certificate including ALC_PAM.1

- genua: genugate 10.0 Z

  The TOE genugate 10.0 Z is a combination of an application level gateway (ALG) and a packet filter (PFL), which are implemented on two different systems. It is part of a larger product. The firewall genugate 10.0 Z consists of hardware and software. The TOE is part of the shipped software. The operating system is a modified OpenBSD.

Antragsteller / Applicant	genua GmbH Domagkstrasse 7 85551 Kirchheim
Prüfstelle / Evaluation Facility	secuvera GmbH
Prüftiefe / Assurance	EAL4+, ALC_FLR.2, ALC_PAM.1, ASE_TSS.2, AVA_VAN.5
Ausstellungsdatum / Certification Date	22.06.2021

Source: BSI Website

- How to apply: practical considerations
  - Strong recommendation: Review existing PAM Processes
    - Check maturity of PAM Processes
    - e.g. Gap-Analysis
    - might help if Security Development Lifecycle (SDL) is already implemented
  - consider ALC_PAM.1 requirements
    - see Guidance in ISO Document (→ Annex)

jtsec
BEYOND IT SECURITY

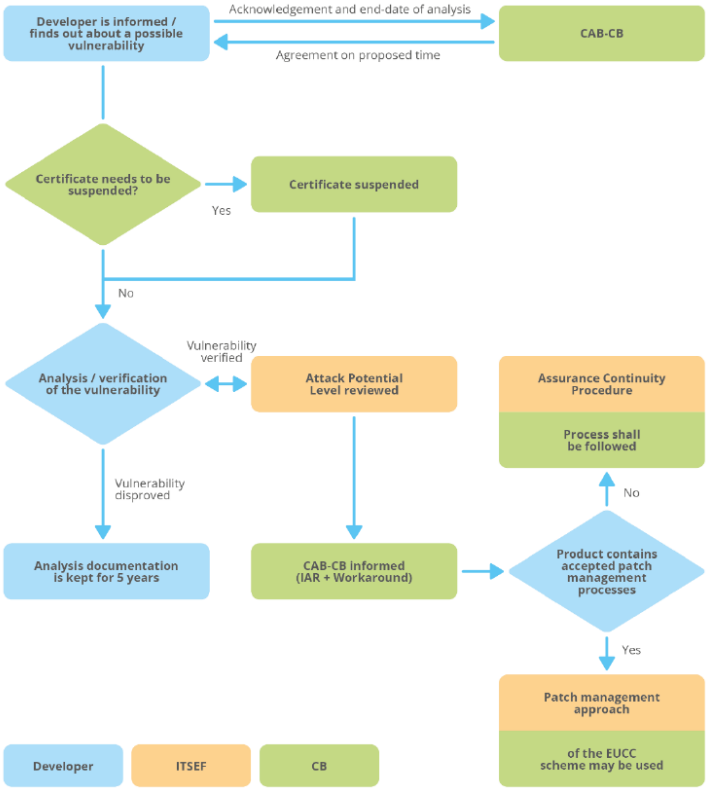
secuvera

Implications of Patch Management in the EUCC Scheme

- Implications of Patch Management in the EUCC Scheme

- Cyber Security Act:
  - (40) ENISA should contribute to raising the public's awareness […] and to **promote** basic multi-factor authentication, **patching**, encryption, anonymisation and data protection advice.
  - (93) European cybersecurity certificates and EU statements of conformity should help end users to make informed choices. […] namely **for how long the end user can expect to receive cybersecurity updates or patches** […]
  - Article 54.1 A European cybersecurity certification scheme shall include at least the following elements: […]
    - **(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with; […]**

- Implications of Patch Management in the EUCC Scheme
  - One year since the publication of EUCC v1.1.1
  - Chapter **14. Rules related to handling vulnerabilities** implements the rules concerning how previously undetected cybersecurity vulnerabilities in ICT products are to be reported and dealt with (Art 54.1m) and provides the hook for patch management.

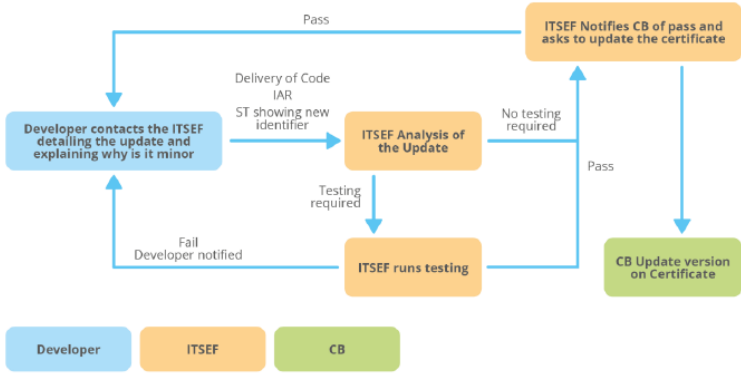


- Patch levels
  - The CB shall include in the certification report the applied Patch management mechanism and a clear delineation of the TOE scope (specially when it is part of a bigger product)

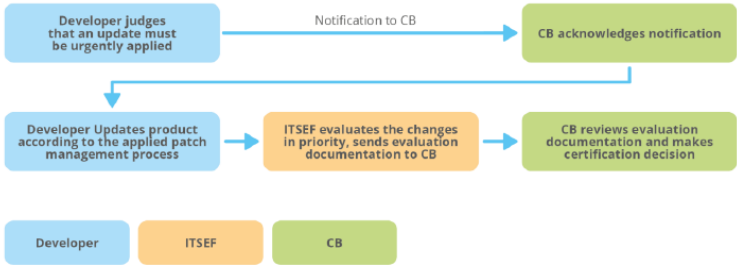
Proximity or availability of the possible attack	Level of change needed to be applied	Patch levels applicable
Attack is available and can be exploited (exploitable vulnerability)	Outside of the TOE	Level 1
	Minor	Critical Update Flow/Level 2
	Major	Critical Update Flow/Level 3
Vulnerability that can be used to develop an attack (exploitable or potential vulnerability)	Outside of the TOE	Level 1
	Minor	Level 2 with potentially Critical Update Flow
	Major	Level 3 with potentially Critical Update Flow
Vulnerability where an attack is not likely or cannot be used for development of an attack potential or residual vulnerability)	Outside of the TOE	Level 1
	Minor	Level 2
	Major	Level 3

  - L1: Just notify CAB-CB and proceed to deploy. CAB may apply maintenance / release a maintenance report.
  - L2: Evaluate and then deploy. CAB shall update the version of the certificate.
  - L3: Fallback to assurance continuity for major changes.
  - CUF: Notify the CAB, then deploy, then evaluate. CAB shall update the version of the certificate.

- Patch levels
  - Level 2
  - A time limit for evaluation may be agreed
    - Would require a contract with the ITSEF
  - It is possible to avoid testing based on the evidence provided (e.g. source code)
  - May not require approval to start from the CB
  - Bug fixes shall be considered typical minor changes



- Patch levels
  - Critical Update Flow

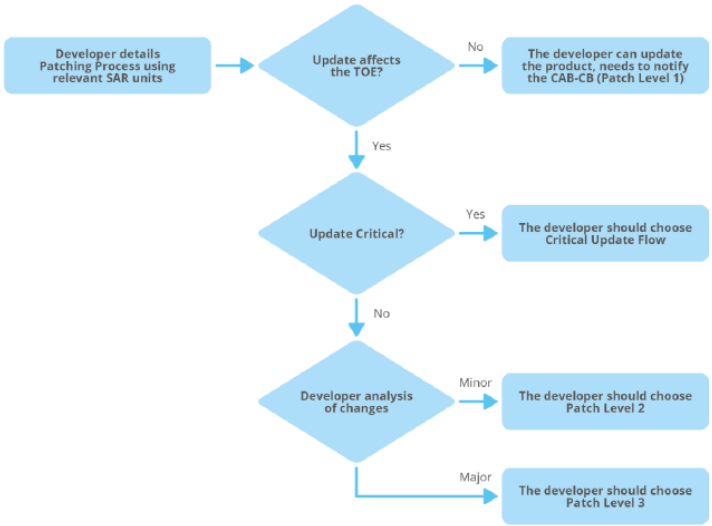


  - Will not require approval to start from the CB but the ITSEF and the CB shall be informed of the changes within five business days.
  - ITSEF shall have a priority queue
    - Would require a contract with the ITSEF
  - Will require validation from the CB

- Critical update flow triage
  - The following questions shall be answered
    - Is the product used within critical infrastructure?
    - Are there applicable liability issues?
    - Is safety at risk?
    - Is a working exploit available or even not needed?
    - Can the vulnerability be used to develop further attacks?

- Practical application
  - When a vulnerability is verified and the patch management was included in the initial evaluation the following steps will be done:
    - 1. Developer notifies the CAB and sends IAR
    - 2. Developer triages the severity of the vulnerability to determine if the Critical Update Flow is applicable.
    - 3. Developer determines the applicable patch level based on the affected evidence (major/minor)
    - 4. The following steps are done in different order depending on the level
      - Deploy the patch
      - Evaluate the patched TOE

      or classical assurance continuity (PL2)
    - 5. A maintenance report is emitted and certificate is updated



- EUCC Next Steps
  - We gained experience through the experiment conducted by Secuvera and BSI
  - Experience for other approaches may be needed (ISCI approach)
  - Further refinement under EUCC for the patch management chapter may be needed, including:
    - Harmonized interpretation of Major/Minor changes for vulnerabilities
    - Consider applying more widely the asynchronous approach. To which extent shall we require ITSEF/CB involvement?
    - Detail the triage process
    - Tuning with other aspects like vulnerability handling and monitoring?
    - There is some potential overlap/contradictions with assurance continuity and with Chapter 12
    - Impact on EUCC ENISA website (certificate list)?

- Conclusions
  - ISO project status
    - next draft for distribution in ISO 1st of July
      - next ballot: DTS (Draft Technical Specification)
      - *ask your ISO liasion organisation for the document, like CCUF*
    - official project target: 2023-04-25
  - On the EUCC Patch Management approach
    - Accepted for trial use opening the door to asynochronus evaluation alternatives
    - Further refinement is still needed

jtsec

BEYOND IT SECURITY

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Thank you!
Vielen Dank!
¡Muchas Gracias!

Javier Tallón
jtallon@jtsec.es
+34-858981999

jtsec Beyond IT Security
Avenida de la Constitución 20, 208
18012 Granada
Spain

Sebastian Fritsch
sfritsch@secuvera.de
+49-7032/9758-24

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden/Stuttgart
Germany