Willkommen

Von Security by Design, Demut und vom Nutzen handwerklicher Qualitäten

PHOENIX CONTACT
INSPIRING INNOVATIONS

Kurzvorstellung Phoenix Contact

Dr. Lutz Jänicke – Corporate Product & Solution Security Officer

- 2002-2015 Innominate Security Technologies AG (jetzt: Phoenix Contact Cyber Security GmbH)
  - CTO; IT-Sicherheitsbeauftragter
- 2016- Corporate Product & Solution Security Officer
  - Phoenix Contact Gruppe/Digital Processes & Solutions
- Plattform Industrie 4.0
  - AG **Sicherheit vernetzter Systeme**; UAG Sichere Kommunikation für Industrie 4.0
- DKE
  - **UK 931.1 IT-Sicherheit in der Automatisierungstechnik (→ IEC 62443)**
  - TBKON Cybersecurity; TBINK AK „Safety & Security“
  - **Beirat CERT@VDE**
- ZVEI
  - Arbeitskreis Cybersicherheit; Lenkungskreis Industrial Security
- VDMA
  - Arbeitskreis Cybersecurity; Arbeitskreis „Sichere Fernwartung“

PHOENIX CONTACT
INSPIRING INNOVATIONS

Kurzvorstellung Phoenix Contact

Dr. Lutz Jänicke – Corporate Product & Solution Security Officer

- 1982: Abitur
- 1983-1989: TU Berlin: Studium der Elektrotechnik
  - Vertiefungsfach Halbleitertechnik
  - Hauptfächer Theoretische Elektrotechnik, Hochfrequenztechnik, Nachrichtentechnik
- 1989-1994: TU Berlin: Wissenschaftlicher Mitarbeiter mit Lehraufgaben
  - Institut für Elektrische Maschinen
- 1994: TU Berlin:
  - „Finite Elemente Methode mit adaptiver Netzgenerierung für die numerische Berechnung dreidimensionaler elektromagnetischer Felder“
- 1995-2001: BTU Cottbus: Oberingenieur
  - Lehrstuhl für allgemeine Elektrotechnik und numerische Feldberechnung
- 1989-2001(+) Systemadministration UNIX-Workstations etc
- 1993+ Firewall, SSL/TLS, SSH -> Open Source z.B. 1999-2017 Mitglied OpenSSL Dev-Team

Gemeinsam kontinuierliches Wachstum

Unternehmenszentrale und Competence Center

Headquarters
Blomberg | Germany

PHOENIX CONTACT
INSPIRING INNOVATIONS

Gemeinsam kontinuierliches Wachstum

Unternehmenszentrale und Competence Center

Group Center of Competence
Harrisburg | USA

Innovation Center Electronics
Bad Pyrmont | Germany

Group Center of Competence
Nanjing | China

PHOENIX CONTACT
INSPIRING INNOVATIONS

Über
100.000
innovative
Produkte

PHOENIX CONTACT
INSPIRING INNOVATIONS

Unternehmensstruktur

Group Functions

Core Business Areas

Device Connectors

Industrial Components and Electronics

Industry Management and Automation

New Business Fields

Innovations- und Start-up-Kultur

INSPIRING INNOVATIONS

Empowering the All Electric Society

Digitalisierung mit Smart Industry Solutions

PHOENIX CONTACT
INSPIRING INNOVATIONS

Praktische Erfahrungen

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

CISA.gov | Services | Report

Alerts and Tips | Resources | Industrial Control Systems

Industrial Control Systems > ICS-CERT Advisories > Innominate MGuard Weak HTTPS and SSH Keys

ICS Advisory (ICSA-12-167-01)

More ICS-CERT Advisories

Innominate MGuard Weak HTTPS and SSH Keys

Original release date: June 15, 2012 | Last revised: September 06, 2018

Print | Tweet | Send | Share

Overview

An independent research group comprised of Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman identified an insufficient entropy vulnerability in Innominate's mGuard network appliance product line. By impersonating the device, an attacker can obtain the credentials of administrative users and potentially perform a Man-in-the-Middle (MitM) attack. Innominate has validated the vulnerability and produced an update that resolves the reported vulnerability. This vulnerability can be remotely exploited.

ICS-CERT has coordinated this vulnerability with Innominate, which has produced an update that resolves this vulnerability.

https://www.cisa.gov/uscert/ics/advisories/ICSA-12-167-01

PHOENIX CONTACT INSPIRING INNOVATIONS

Bug 11152 - receiving an SMS with a printf format string will crash gsm tool

Status: VERIFIED FIXED (edit)

Product: mGuard
Component: mguard-console
Version: 8.0.0
Platform: PC Linux

Importance: P1 blocker
Target Milestone: Release 8.0.1

[redacted] 2013-07-31 12:57:02 CEST Description [reply] [-]

```
In atparse.y,

static int write_eds(const char *path, const char *value)

is used among other things to write SMS message texts to the EDS, which will call

snprintf(edsAtt.value, EDS_VALUE_MAXLEN, value)

which will segfault the gsm-tool daemon if the message text contains any printf
format strings.

The daemon will keep restarting and crashing indefinitely.
```

[redacted] 2013-07-31 14:18:22 CEST Comment 1 [reply] [-]

```
commit 2b54d21bd97d23c5166560ee7934ce7ea38f4229
Author: [redacted]
Date:   Wed Jul 31 13:51:40 2013 +0200

    bug#11152 receiving an SMS with a printf format string will crash gsm tool

    don't use snprintf to write SMS message string to EDS attribute value
```

Bug 14913 - handle 'kissing face with smiling eyes' and other surrogates more gracefully in encode_utf8()

Status: RESOLVED FIXED (edit)

Reported: 2015-07-(

Modified: 2015-09-

CC List: ☐ Add m

5 users (

Product: mGuard

Component: mguard

Version: 8.3.0-pre16

Platform: PC Linux

Importance: P3 normal

Target Milestone: Release 8.3.0

[redacted] 2015-07-02 17:56:38 CEST Description [reply] [-]

```
mguard1 at the PxC USA test lab (Running on 3G, DTAG USA) kept restarting gsm-tool.

Apparently, we received a message labeled as DCS2-encoded.

It turned out encode_utf8() exited because of a "too high code point", and gsm-tool
asserted, because assuming that a DCS2-encoded message does not contain surrogates
(and by definition it shouldn't).

However, the message did contain a surrogate. I don't know who sent it, but it
decodes as 'Hello<U+1F619>', Unicode Character 'KISSING FACE WITH SMILING EYES'.

http://www.fileformat.info/info/unicode/char/1f619/index.htm

My speculation is that verizon cdma sends 'real' UTF16, while gsm assumes the more
restricted and deprecated DCS2.

input unicode: 0:48 1:65 2:6c 3:6c 4:6f 5:d83d 6:de19 INITIAL: len: 7, utf8len: 0,
flags: 0ERR: utf16 surrogate: d83d
COULD NOT ENCODE TO UTF8
pdu_mock: /home/sedel/mguard/mguard-console/src/pdu.c:457: parse_pdu: Assertion `0'
failed.
Aborted
```

[redacted] 2015-07-27 16:33:05 CEST Comment 1 [reply] [-]

```
commit c83fe1993c391065e95265fb62024507506d2d19
Author: [redacted]
Date:   Thu Jul 2 16:03:53 2015 +0200

    Bug 14913 - handle 'kissing face with smiling eyes' and other surrogates mor

    * transform utf16 surrogates, drop unpaired surrogates
    * also eliminate assertions from pdu.c
    * also terminate output string on U+0
```

[redacted] 2015-09-21 12:53:56 CEST Comment 2 [reply] [-]

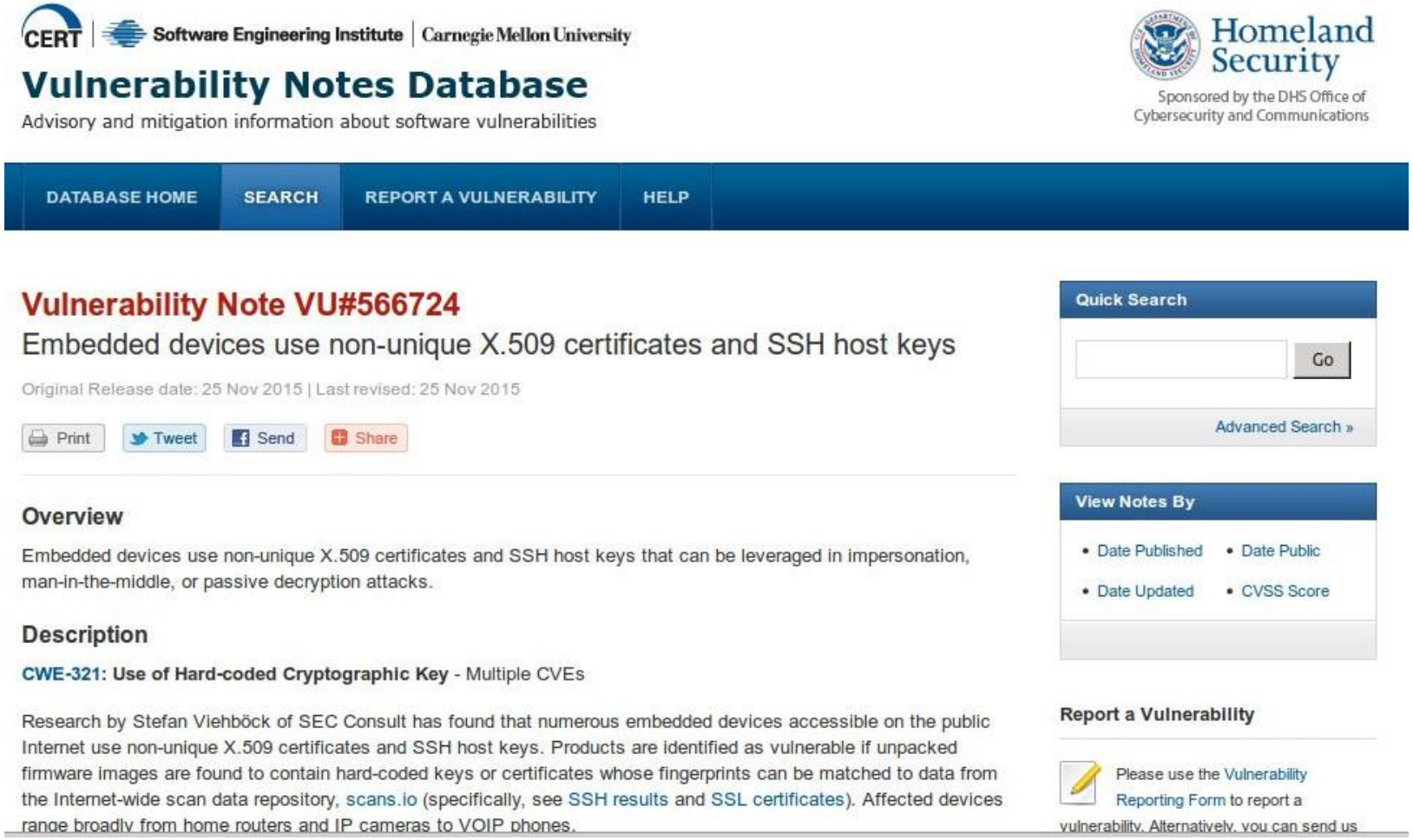
will verify

[redacted] 2015-09-21 14:28:32 CEST Comment 3 [reply] [-]

This is very hard to reproduce because according to the 3G specification no UTF16 surrogates should arrive at a 3G device. An unknown phone user with an unknown provider sent this message to T-Mobile(USA) and either T-Mobile or that unknown other provider did not conform to the 3G standard and did not filter out the surrogate (typically and as observed by [redacted] it is replaced with a '?').

Suggest code review for verification.

„House of Keys“ (2015)



CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Homeland Security

Sponsored by the DHS Office of Cybersecurity and Communications

DATABASE HOME | SEARCH | REPORT A VULNERABILITY | HELP

Vulnerability Note VU#566724

Embedded devices use non-unique X.509 certificates and SSH host keys

Original Release date: 25 Nov 2015 | Last revised: 25 Nov 2015

Print | Tweet | Send | Share

Overview

Embedded devices use non-unique X.509 certificates and SSH host keys that can be leveraged in impersonation, man-in-the-middle, or passive decryption attacks.

Description

CWE-321: Use of Hard-coded Cryptographic Key - Multiple CVEs

Research by Stefan Viehböck of SEC Consult has found that numerous embedded devices accessible on the public Internet use non-unique X.509 certificates and SSH host keys. Products are identified as vulnerable if unpacked firmware images are found to contain hard-coded keys or certificates whose fingerprints can be matched to data from the Internet-wide scan data repository, scans.io (specifically, see SSH results and SSL certificates). Affected devices range broadly from home routers and IP cameras to VOIP phones.

Quick Search

Go

Advanced Search »

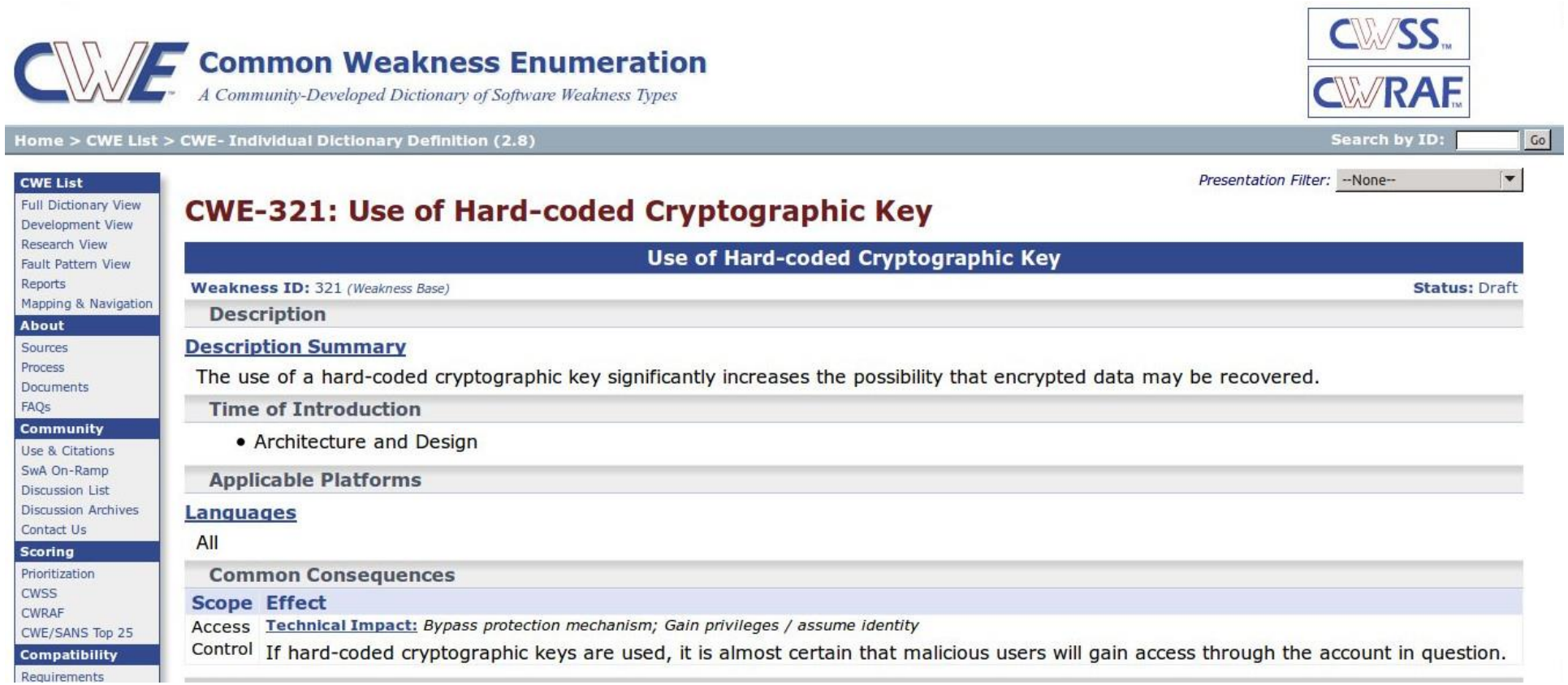
View Notes By

- Date Published
- Date Public
- Date Updated
- CVSS Score

Report a Vulnerability

Please use the Vulnerability Reporting Form to report a vulnerability. Alternatively, you can send us

„House of Keys“ (2015)



Common Weakness Enumeration
A Community-Developed Dictionary of Software Weakness Types

CWSS
CWRAF

Home > CWE List > CWE- Individual Dictionary Definition (2.8)

Search by ID: Go

CWE List
Full Dictionary View
Development View
Research View
Fault Pattern View
Reports
Mapping & Navigation
About
Sources
Process
Documents
FAQs
Community
Use & Citations
SwA On-Ramp
Discussion List
Discussion Archives
Contact Us
Scoring
Prioritization
CWSS
CWRAF
CWE/SANS Top 25
Compatibility
Requirements

Presentation Filter: --None--

CWE-321: Use of Hard-coded Cryptographic Key

Use of Hard-coded Cryptographic Key

Weakness ID: 321 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered.

Time of Introduction

- Architecture and Design

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Access Control	**Technical Impact:** *Bypass protection mechanism; Gain privileges / assume identity* If hard-coded cryptographic keys are used, it is almost certain that malicious users will gain access through the account in question.

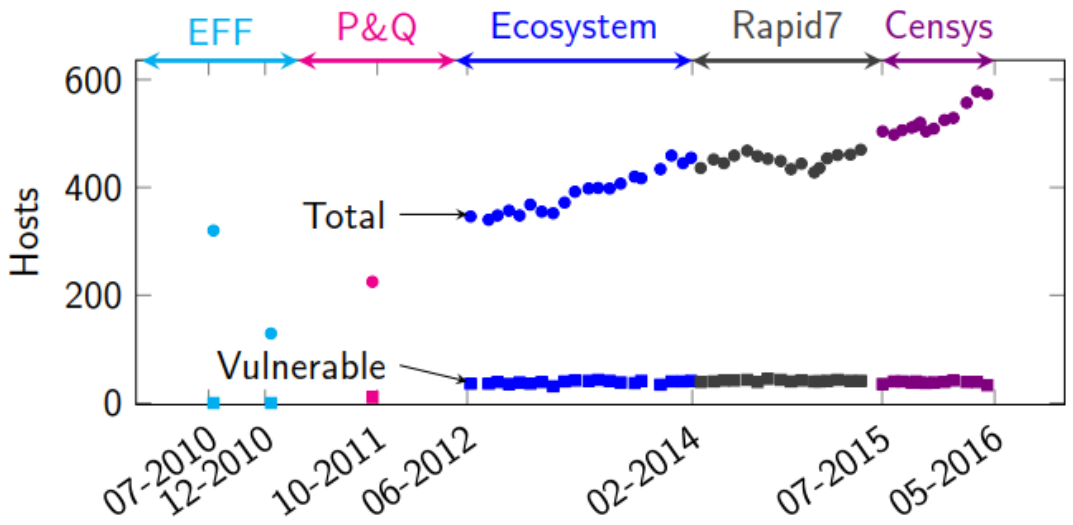
https://cwe.mitre.org/data/definitions/321.html

Weak keys revisited (2016)

Innominate

mGuard network security devices (Smart, PCI, Industrial RS, Blade, Delta, EAGLE)

- Public advisory in June 2012
- Consistent population of vulnerable devices since 2012
- New devices not vulnerable, but old devices not patched



Source: https://www.ietf.org/proceedings/98/slides/slides-98-maprg-weak-keys-remain-widespread-in-network-devices-marcella-hastings-00.pdf

07 June 2021
300505868

Security Advisory for FL SWITCH SMCS series

Advisory Title

Multiple vulnerabilities have been discovered in the current firmware of the PHOENIX CONTACT FL SWITCH SMCS series switches.

Advisory ID

CVE-2021- 20003
CVE-2021- 20004
CVE-2021- 20005
VDE-2021-023

Vulnerability Description

TCP-Fragmentation DoS vulnerability (CVE-2021- 20003, CWE-404):
Fragmented TCP-Packets may cause a Denial of Service of Web-, SNMP-, and ICMP Echo-service. The switching functionality of the device is not affected.

LLDP XSS vulnerability (CVE-2021- 20004, CWE-79):
An attacker may insert malicious code via LLDP frames into the web-based management which could then be executed by the client.

Urgent-Flag DoS vulnerability (CVE-2021- 20005, CWE-362):
If an attacker sends a hand-crafted TCP-Packet with the Urgent-Flag set and the Urgent-Pointer set to 0, the network stack will crash. The device needs to be rebooted afterwards.

10 November 2021
300524757

Security Advisory for FL MGUARD 1102/1105

Advisory Title

Cross-site scripting in web-based management and memory leak in the remote logging function of FL MGUARD 1102 and FL MGUARD 1105

Advisory ID

CVE-2021-34582
CVE-2021-34598
VDE-2021-046

Vulnerability Description

CVE-2021-34582:
The file upload functionality in the web-based management is affected by a stored cross-site scripting vulnerability (CWE-79: Improper Neutralization of Input During Web Page Generation).

An authenticated FL MGUARD user with *Admin* or *Super Admin* role can upload a certificate file on the **Basic settings > LDAP** page, on the **Logs > Remote logging** page, or through the REST API. The content of this file is embedded into the corresponding web page, and any HTML code within the file is rendered when the page is viewed by the same or a different authenticated user.

CVE-2021-34598:
The remote logging functionality is impaired by the lack of memory release for data structures from syslog-ng when remote logging is active (CWE-770: Allocation of Resources Without Limits or Throttling).

25 January 2022
300537202

Security Advisory for FL SWITCH 2xxx series

Advisory Title

An unprivileged user connected via SSH Command Line Interface (CLI) gains admin privileges.

Advisory ID

CVE-2022-22509
VDE-2022-001

Vulnerability Description

The user management of the FL SWITCH 2xxx family of devices implements access rights based on roles and permission groups. An unprivileged user logged in via the SSH CLI is assigned to the admin role independent of his configured access role enabling full access to the device configuration (CWE-266 - Incorrect Privilege Assignment).

Affected products

User Management via SSH was first introduced with firmware version 3.00. Firmware versions other than 3.00 are not affected by this vulnerability.

Weak keys (CWE-321) 2021

Weak SSH Key Generation Fix in GitKraken v8.0.1

GitKraken

October 11, 2021

If you are using GitKraken versions 7.6.x, 7.7.x, or 8.0.0, this article explains what steps you can take to maintain secure SSH key connections to remote repositories on GitHub, GitLab, Bitbucket, and Azure DevOps.

How to Fix the Weak SSH Key Issue

This issue only affects GitKraken users who generated SSH keys through the GitKraken interface using versions 7.6.x, 7.7.x, 8.0.0. If you are not sure what version you used to generate your SSH key, we encourage you to renew your key through the following process.

Affected users need to:

1. Remove all old GitKraken-generated SSH keys stored locally.

2. Generate new SSH keys using GitKraken 8.0.1, or later, for each of your Git service providers.

https://www.gitkraken.com/blog/weak-ssh-key-fix

CWE VIEW: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses

1337 - Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses

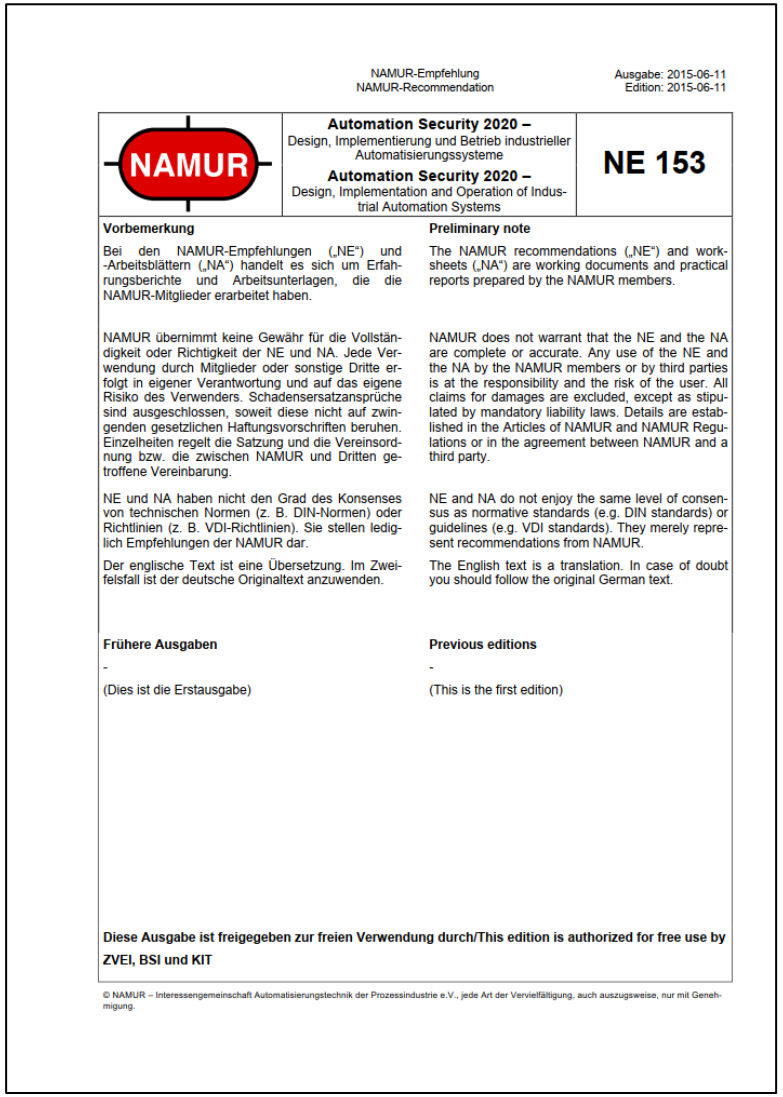
- Out-of-bounds Write - *(787)*
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - *(79)*
- Out-of-bounds Read - *(125)*
- Improper Input Validation - *(20)*
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - *(78)*
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - *(89)*
- Use After Free - *(416)*
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - *(22)*
- Cross-Site Request Forgery (CSRF) - *(352)*
- Unrestricted Upload of File with Dangerous Type - *(434)*
- Missing Authentication for Critical Function - *(306)*
- Integer Overflow or Wraparound - *(190)*
- Deserialization of Untrusted Data - *(502)*
- Improper Authentication - *(287)*
- NULL Pointer Dereference - *(476)*
- Use of Hard-coded Credentials - *(798)*
- Improper Restriction of Operations within the Bounds of a Memory Buffer - *(119)*
- Missing Authorization - *(862)*
- Incorrect Default Permissions - *(276)*
- Exposure of Sensitive Information to an Unauthorized Actor - *(200)*
- Insufficiently Protected Credentials - *(522)*
- Incorrect Permission Assignment for Critical Resource - *(732)*
- Improper Restriction of XML External Entity Reference - *(611)*
- Server-Side Request Forgery (SSRF) - *(918)*
- Improper Neutralization of Special Elements used in a Command ('Command Injection') - *(77)*

http://cwe.mitre.org/data/definitions/1337.html

Security by Design

„Security by Design“

- **Security by Design** als „stehender Begriff“?
- NAMUR Empfehlung 153 (2015): Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme
  - Security by Design
  - Security by Implementation
  - Security by Default
  - Secure in Deployment



NAMUR-Empfehlung
NAMUR-Recommendation

Ausgabe: 2015-06-11
Edition: 2015-06-11

NAMUR

Automation Security 2020 –
Design, Implementierung und Betrieb industrieller Automatisierungssysteme
Automation Security 2020 –
Design, Implementation and Operation of Industrial Automation Systems

NE 153

Vorbemerkung

Bei den NAMUR-Empfehlungen („NE“) und -Arbeitsblättern („NA“) handelt es sich um Erfahrungsberichte und Arbeitsunterlagen, die die NAMUR-Mitglieder erarbeitet haben.

NAMUR übernimmt keine Gewähr für die Vollständigkeit oder Richtigkeit der NE und NA. Jede Verwendung durch Mitglieder oder sonstige Dritte erfolgt in eigener Verantwortung und auf das eigene Risiko des Verwenders. Schadensersatzansprüche sind ausgeschlossen, soweit diese nicht auf zwingenden gesetzlichen Haftungsvorschriften beruhen. Einzelheiten regelt die Satzung und die Vereinsordnung bzw. die zwischen NAMUR und Dritten getroffene Vereinbarung.

NE und NA haben nicht den Grad des Konsenses von technischen Normen (z. B. DIN-Normen) oder Richtlinien (z. B. VDI-Richtlinien). Sie stellen lediglich Empfehlungen der NAMUR dar.

Der englische Text ist eine Übersetzung. Im Zweifelsfall ist der deutsche Originaltext anzuwenden.

Frühere Ausgaben

-

(Dies ist die Erstausgabe)

Preliminary note

The NAMUR recommendations („NE“) and worksheets („NA“) are working documents and practical reports prepared by the NAMUR members.

NAMUR does not warrant that the NE and the NA are complete or accurate. Any use of the NE and the NA by the NAMUR members or by third parties is at the responsibility and the risk of the user. All claims for damages are excluded, except as stipulated by mandatory liability laws. Details are established in the Articles of NAMUR and NAMUR Regulations or in the agreement between NAMUR and a third party.

NE and NA do not enjoy the same level of consensus as normative standards (e.g. DIN standards) or guidelines (e.g. VDI standards). They merely represent recommendations from NAMUR.

The English text is a translation. In case of doubt you should follow the original German text.

Previous editions

-

(This is the first edition)

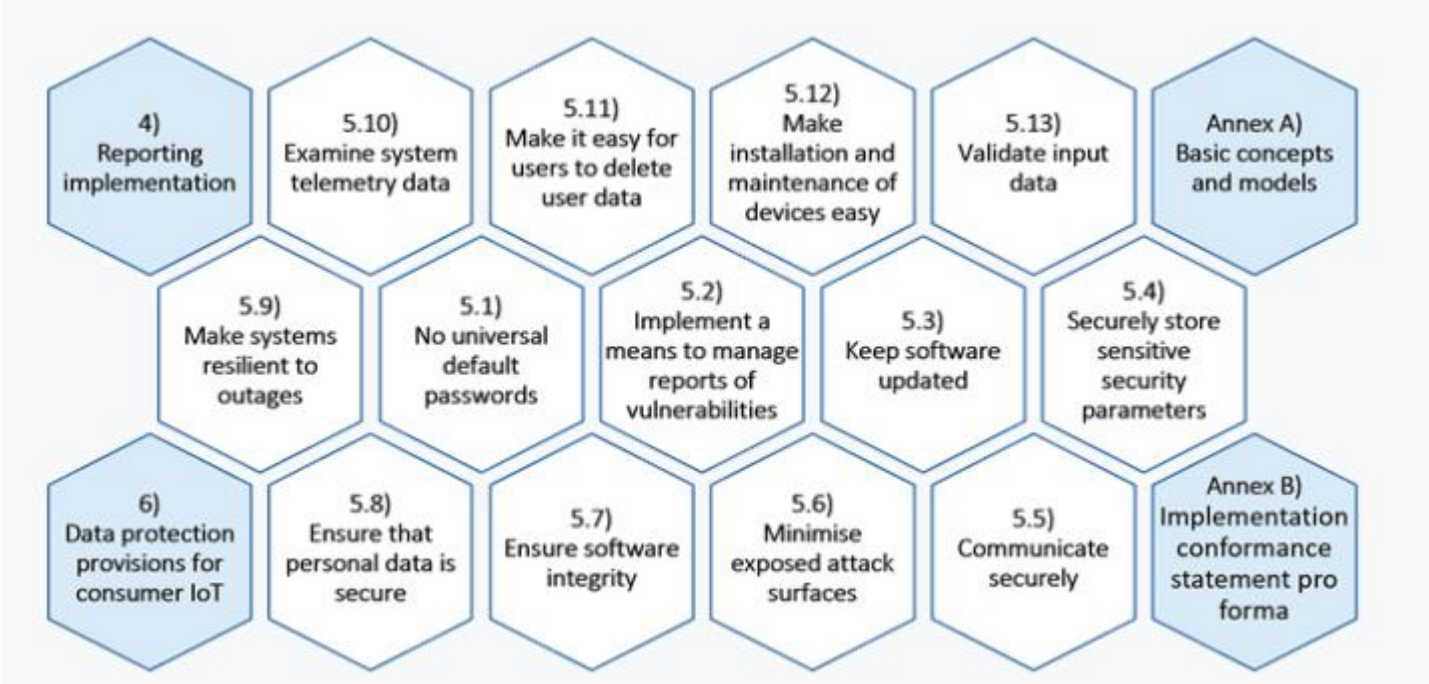
Diese Ausgabe ist freigegeben zur freien Verwendung durch/This edition is authorized for free use by ZVEI, BSI und KIT

ETSI EN 303 645 V2.1.1 (2020-06)

CYBER;
Cyber Security for Consumer Internet of Things:
Baseline Requirements

ETSI TS 103 701 V1.1.1 (2021-08)

CYBER;
Cyber Security for Consumer Internet of Things:
Conformance Assessment of Baseline Requirements



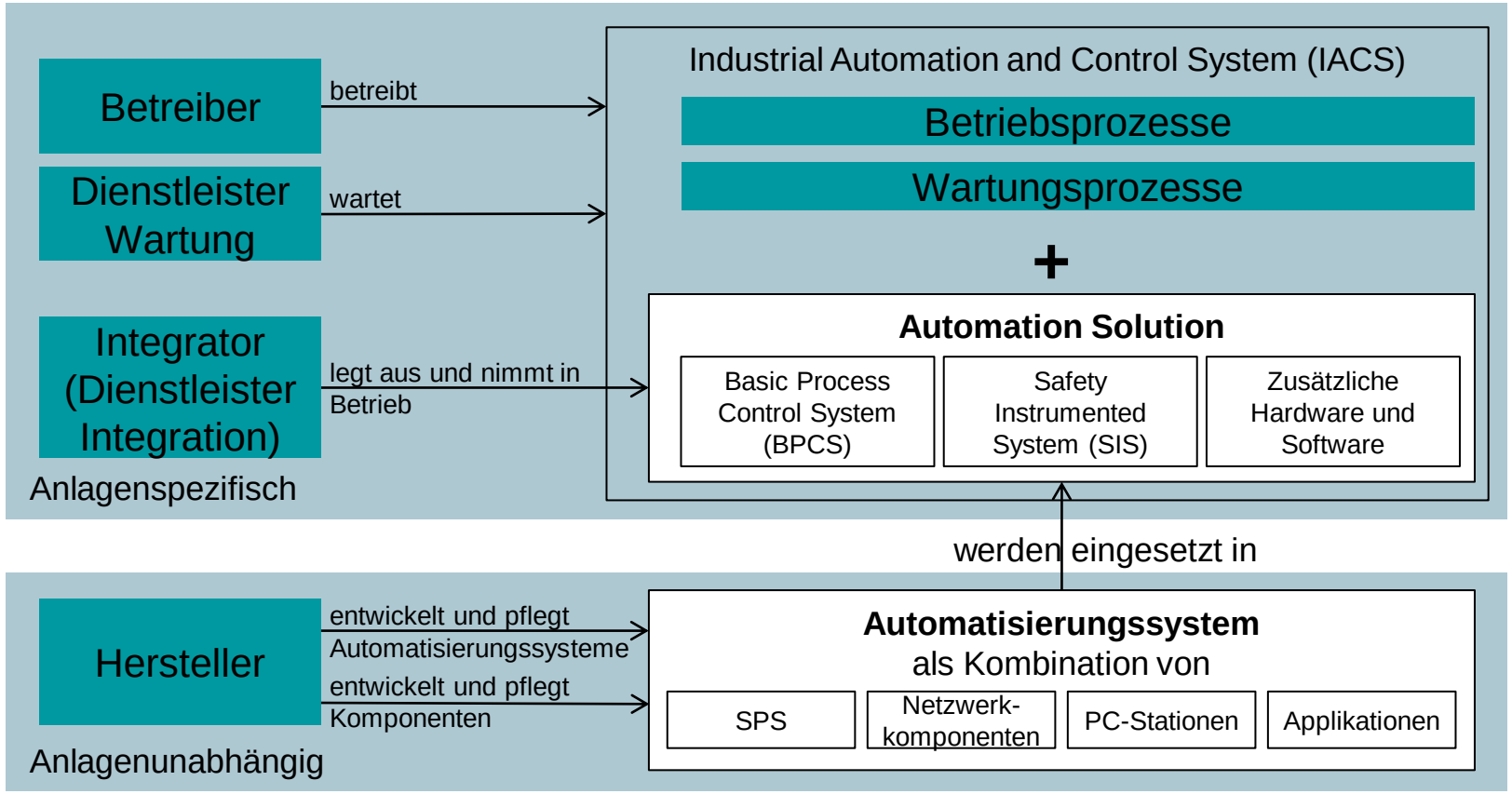
https://www.etsi.org/technologies/consumer-iot-security

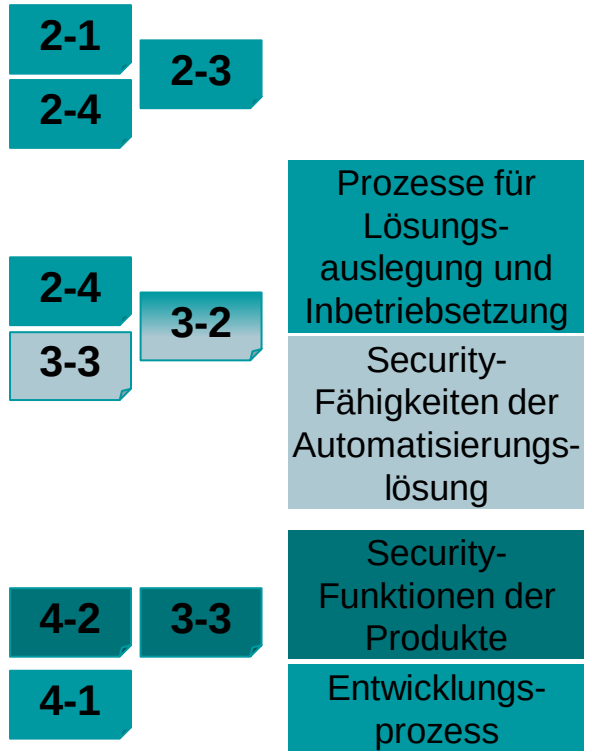
IEC 62443: Erweiterte Struktur

General	Policies and procedures	System	Component	Profiles	Evaluation
1-1 Technology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS (TR)	4-1 Secure product development lifecycle		6-1 Security evaluation methodology for IEC 62443 – Part 2-4 (TS)
1-2 Master Glossary of terms and abbreviations	2-2 Security Protection Rating	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS products		6-2 Security evaluation methodology for IEC 62443 – Part 4-2 (TS)
1-3 System security compliance metrics	2-3 Patch management in the IACS environment (TR)	3-3 System security requirements and security levels			
1-4 System security lifecycle and use case	2-4 Requirements for IACS solution suppliers				
1-5 Rules for IEC 62443 Profiles (TS)	2-5 Implementation Guidance for IACS Asset Owners				
Definitions Metrics	Security Requirements for plant owner and suppliers	Security Requirements for a secure system	Security Requirements for secure components	Profiles for IACS solution suppliers (and more?)	Evaluation methodologies for conformity assessment

Process requirements ***Functional requirements***

Basisrollen in der IEC 62443





IEC 62443-4-2

- **FR1 IAC - Identifizierung und Authentifizierung**
  Alle Nutzer (menschliche Nutzer, Softwareprozesse und Geräte) identifizieren und authentifizieren
- **FR2 UC – Nutzungskontrolle**
  Authentifizierten Nutzern zugewiesenen Berechtigungen werden durchgesetzt und überwacht (autorisiert)
- **FR3 SI – Systemintegrität**
  Integrität der Komponente sicherstellen und nicht autorisierte Manipulation verhindern
- **FR4 DC - Vertraulichkeit der Daten**
  Vertraulichkeit von Daten bei der Übertragung und auf Speichermedien sicherstellen
- **FR5 RDF - eingeschränkter Datenfluss**
  Automatisierungssysteme in Zonen und Conduits aufteilen, um unnötigen Datenfluss zu verhindern
- **FR6 TRE - rechtzeitige Reaktion auf Ereignisse**
  Auf IT-Sicherheitsverstöße durch Benachrichtigen, Beibringen von Beweisen mit rechtzeitigen Maßnahmen reagieren
- **FR7 RA - Verfügbarkeit der Ressourcen**
  Verfügbarkeit der Anwendungen gegen den Ausfall oder die Verschlechterung wesentlicher Dienste sicherstellen

IEC 62443 4-2 Ausgewählte Komponenten Anforderungen

- **CR 1.7 Stärke der Authentifikation durch Passwörter (SL 1)**
  Passwortregeln mit Zeitbegrenzung
- **CR 1.11 Erfolglose Anmeldeversuche (SL 1)**
  Anzahl der erfolglosen Anmeldeversuche mit Zeitsperre
- **CR 1.12 Nutzungshinweis (SL 1)**
  Informationen und Warnungen Datenschutz und zur IT-Sicherheit
- **CR 2.8 - 13 Prüfbare Ereignisse (SL1/2/3)**
  Security Event Logging mit Zeitstempel und API zum systemweiten Speichern
- **EDR 3.12/13 Bereitstellung von Vertrauensankern (SL 2)**
  Hersteller und Betreiber

IEC 62443-4-2 Komponenten industrieller Automatisierungssysteme

Security Levels definieren 56 funktionale Maßnahmen

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 7 – Resource availability (RA)				
CR 7.1 – Denial of service protection	✓	✓	✓	✓
RE (1) Manage communication load from component		✓	✓	✓
CR 7.2 – Resource management	✓	✓	✓	✓
CR 7.3 – Control system backup	✓	✓	✓	✓
RE (1) Backup integrity verification		✓	✓	✓
RE (2) Local backup			✓	✓
CR 7.4 – Control system recovery and reconstitution	✓	✓	✓	✓
CR 7.6 – Network and security configuration settings	✓	✓	✓	✓
RE (1) Machine-readable reporting of current security settings			✓	✓
CR 7.7 – Least functionality	✓	✓	✓	✓
CR 7.8 – Control system component inventory		✓	✓	✓

4.5.1 Software Entwicklungsprozess:

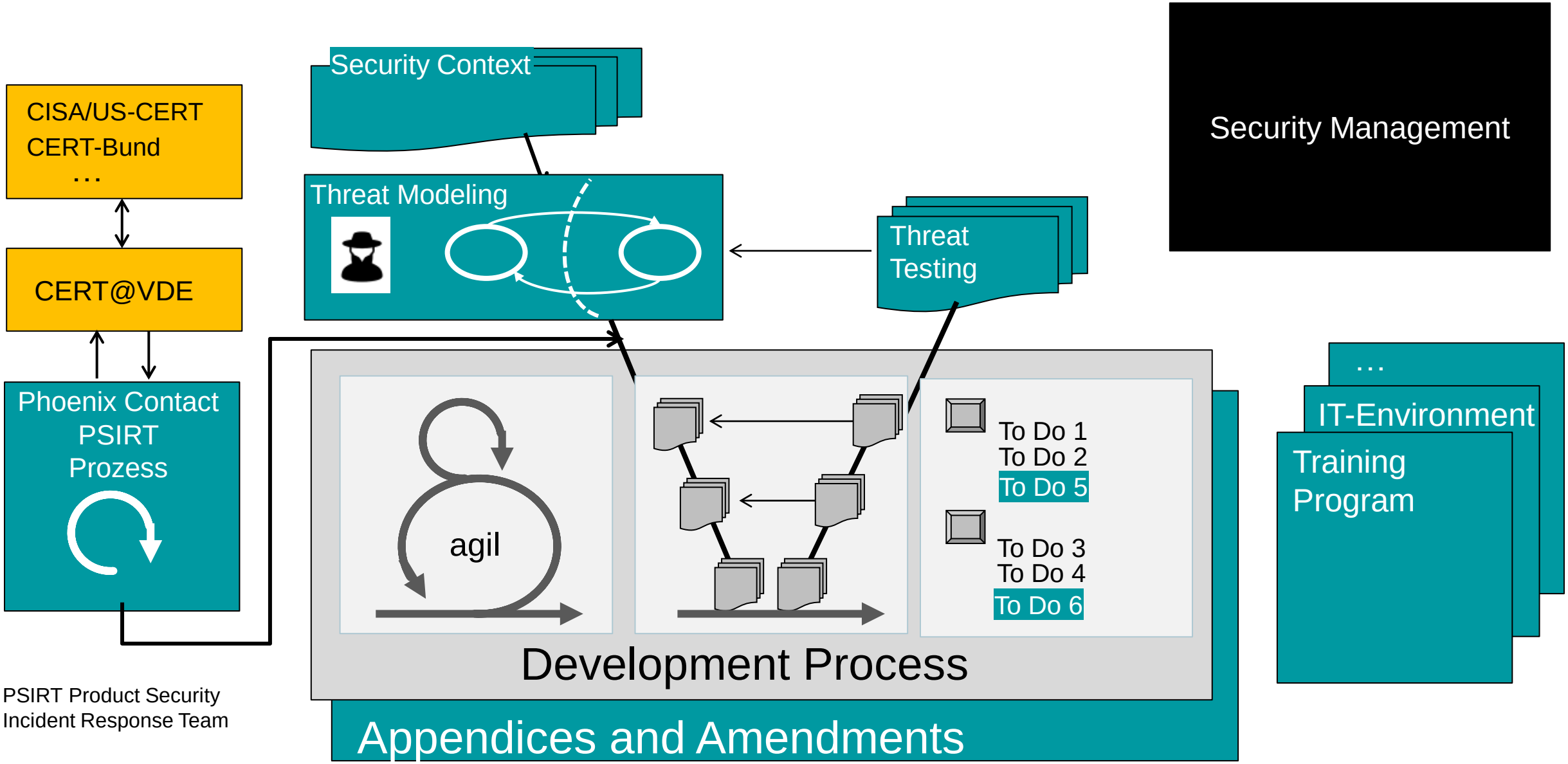
Sämtliche in dieser Norm festgelegten Komponenten (Anforderungen) müssen nach dem in IEC 62443-4-1 beschriebenen Leitfaden für einen Security Produktentwicklungsprozess entwickelt werden.

IEC 62443 4-1 8 Prozessansätze *47 Anforderungen*

1. SM: Verwaltung der IT-Sicherheit
2. SR: Spezifikation der IT-Sicherheitsanforderungen
3. SD: IT-Sicherheit durch den Entwurf
4. SI: Gesicherte Implementierung
5. SVV: Verifikations- und Validierungsprüfung
6. DM: Behandlung von Mängeln in der IT Sicherheit
7. SUM: Verwaltung von IT-Sicherheits-Updates
8. SG: IT-Sicherheitsrichtlinien (Dokumentation)

IEC 62443 4-1 8 Prozessansätze *47 Anforderungen*

SD-1 – Secure Design Principles
SD-2 – Defence in Depth Design
SD-3 – Security Design Review
SD-4 – Secure Design Best Practices
SI-1 – Security Implementation Review
SI-2 – Secure Coding Standards



PSIRT Product Security
Incident Response Team

Wichtigste Anforderungen sind Teil des Security Managements

- SM-11: Assessing and addressing security-related issues
  - A process shall be employed for verifying that a product or a patch is not released until its security-related issues have been addressed and tracked to closure (see 10.5). This includes issues associated with:
    a. requirements (see Clause 6);
    b. secure by design (see Clause 7);
    c. implementation (see Clause 8);
    d. verification/validation (see Clause 9); and
    e. defect management (see Clause 10).
- SM-12: Process verification
  - A process shall be employed for verifying that, prior to product release, all applicable security-related processes required by this specification (see 5.7) have been completed with records documenting the completion of each process.

„Ist eigentlich fertig, stürzt nur noch ab“

„Ich brauche keine Längenprüfung, ich habe das im Griff“

„Ich will kodieren, keine Zeit mit unnützem Formalkram vergeuden“

Manifesto for Agile Software Development

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

That is, while there is value in the items on
the right, we value the items on the left more.

„Documentation is waste“

Software von… bis

1989+: NCSA-Telnet (Freeware für MS DOS)

NCSA PC Telnet Info Page

Note: NCSA Telnet is a **non-supported** product.

Current version is 2.3.08

NCSA Telnet allows a PC running MSDOS on a TCP/IP network to connect to other machines with the telnet protocol. The package includes a Telnet client, an FTP client, and LPR, Setclock, RSH, REXEC, Finger, and Whois utilities. The Telnet client has VT100 support, can open multiple connections, has a scrollback buffer with mouse support, can cut and paste from the scrollback buffer, allows keyboard remapping, uses a packet driver and has internal drivers for some hardware, and emulates a Tektronix 4014.

Documentation (Single .doc file, 168K)

- The readme file
- The FAQ
- Developers notes

PC Telnet is released as a PKZip zipfile, and is located at the NCSA ftp server (as well as many mirror sites). The PKZip archive utility is available here.

- PC Telnet FTP directory
- Binary Distribution *(792K)*
- Source Distribution *(688K)* for Telnet and the included utilities.

Packet Drivers

Telnet now comes with a smaller executable as well which cannot connect without a packet driver. Packet drivers are the standard interface between newer ethernet cards and Telnet anyway. For information on packet drivers contact Crynwr. Packet drivers and utilities can be found at the anonymous ftp site oak.oakland.edu .

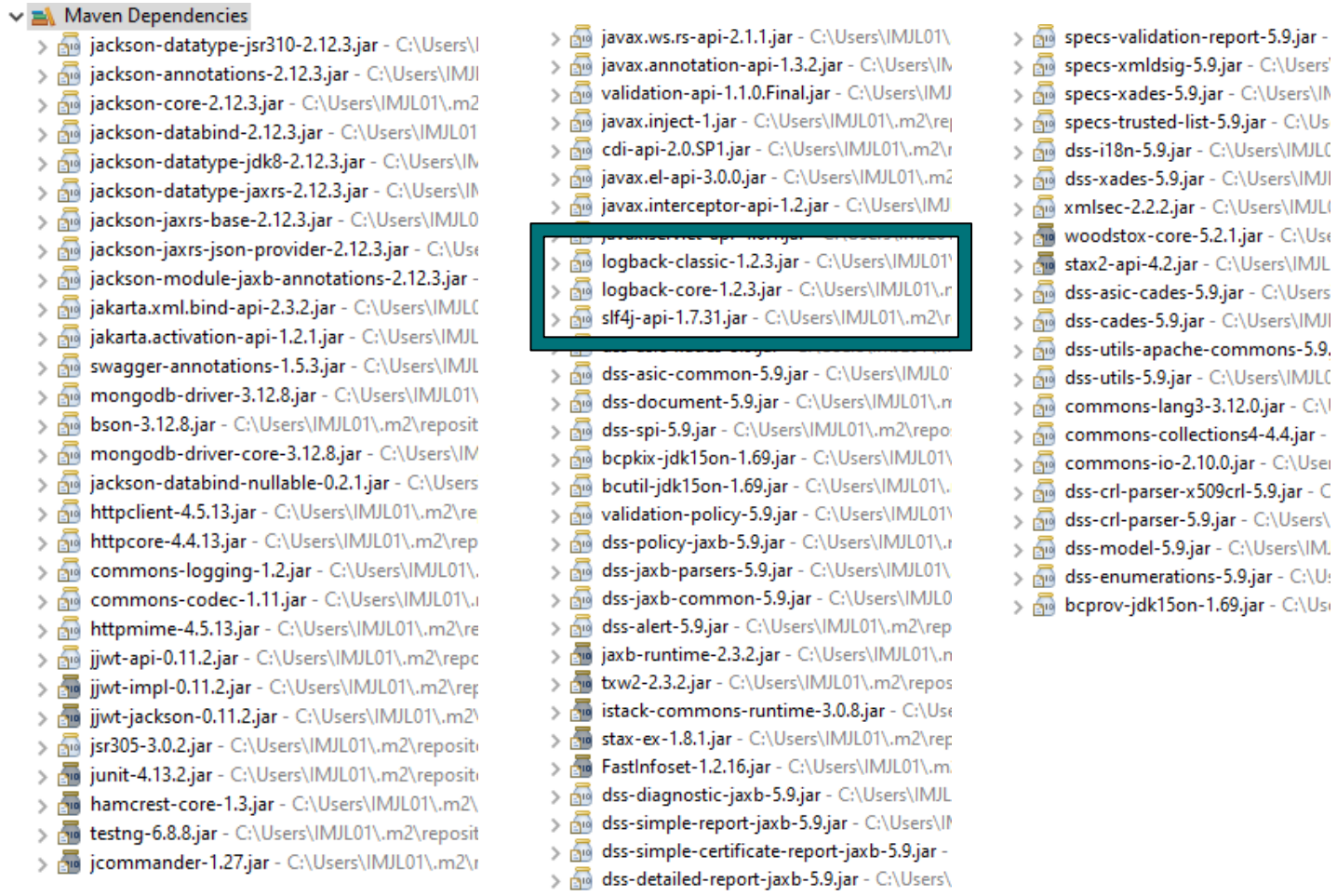
Software Development Division/NCSA

NCSA

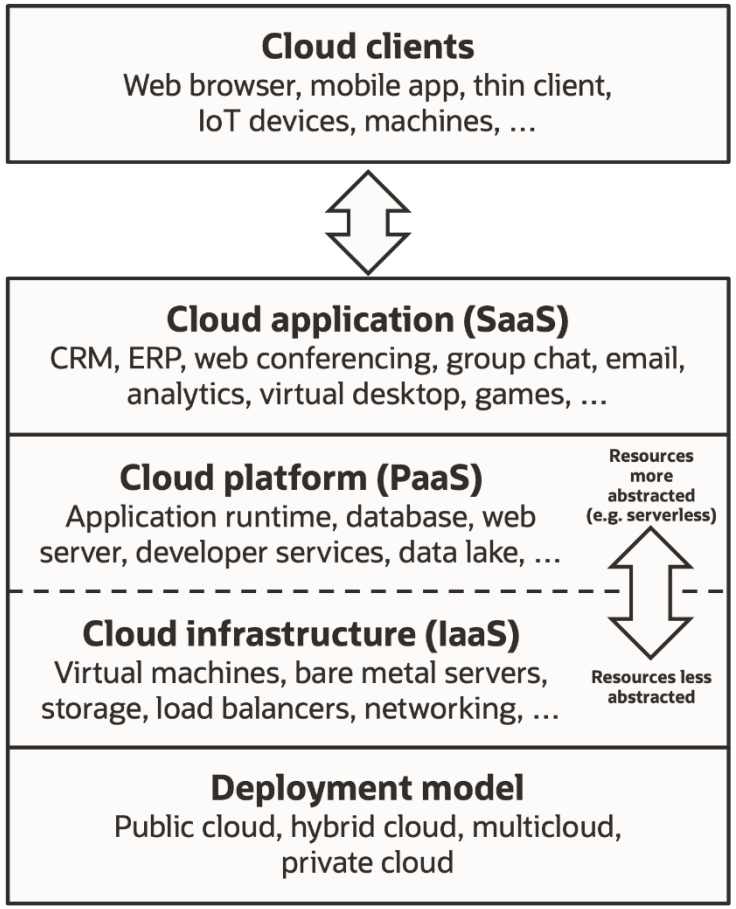
Contact webmaster@ncsa.uiuc.edu with questions regarding this page.
Last updated Sep 28, 2000. All rights reserved.

Quelle: Wayback Machine

2022: Software, frisch gepresst aus unterschiedlichsten Orangen



2022: Läuft ggf. als SaaS auf PaaS in IaaS



https://commons.wikimedia.org/wiki/File:Cloud_computing_service_models_(1).png

Versuch eines Blicks in die Zukunft

Anforderungen heute und morgen

Nationale / Internationale Initiativen

Regulatorien erfüllen

Beschreiben was getan werden muss

Richtlinie zur Netz- und Informationssicherheit

Bundesministerium des Innern

IT Sicherheitsgesetz

Bundesnetzagentur

Sicherheitskatalog

- Meldepflicht für Zwischenfälle
- Aufbau und Zertifizierung eines ISMS
- Erfüllung von technischen Mindestanforderungen, z.B. BDEW

Unabhängige Überprüfung und Abnahme des ICS Systems

Überprüfbare Umsetzung (NERC) für Energieversorgungsanlagen (seit 2010)

Empfehlungen beachten

Beschreiben was getan werden sollte

Bundesamt für Sicherheit in der Informationstechnik

BSI IT-Grundschutzkataloge
ICS-Security Kompendium

BDEW White Paper

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC CIP

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST Cyber Security Framework

Basis-Standards entsprechen

Beschreiben wie es umgesetzt werden sollte

IEC 62443 (System Sicherheit)
IEC 62351 (Kommunikations Sicherheit)
ISO/IEC 27001,27002/19 (Sicherheits Management)

Bundesamt für Sicherheit in der Informationstechnik

BSI Technische Richtlinien

https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/how-european-cyber-resilience-act-will-help-protect-europe_en#:~:text=%20How%20a%20European%20Cyber%20Resilience%20Act%20will,to%20detect%20a%20sophisticated%20attack.%20Then%2C...%20More%20

POSITION | CYBERSECURITY | EU LEGISLATION

EU-wide Cybersecurity Requirements

Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act.

February 1, 2021

BDI Bundesverband der Deutschen Industrie e.V.

DIN

DKE

Introduce horizontally mandatory cybersecurity requirements in accordance with the principles of the New Legislative Framework

Danke

Von Security by Design, Demut und vom Nutzen handwerklicher Qualitäten

PHOENIX CONTACT
INSPIRING INNOVATIONS