Federal Office for Information Security

ERNW providing security.

CWA and CovPass: Two Years of Pandemic-Related Security Assessments

Pascal Jeschke, Health Security Expert – BSI

Dennis Heinze, Security Analyst & Researcher – ERNW

06/29/2022 Heidelberg

Structure

Introduction: BSI

Corona-Warn-App (CWA)

CovPass App

Assessments

Technical Approach

Vulnerability Examples

Federal Office for Information Security

ERNW providing security.

BSI-profil

Foundation
01. Januar 1991

197 Mio. Euro Budget 2021

Positions in 2021

1550 ↗

116 New Positions In 2021

BSI

- Site
- Base
- Liaison office

Section DI 24

Telematik-infrastruktur (TI)

- Health insurance card
- Electronic prescription
- Electronic patient record

Security of medical devices

- Vulnearbility analysis
- Projects

Security incidents

- Cooperation with Federal Institute for Drugs and Medical Devices (BfArM)
- Situation room

IT-Security requirements

- Technical directives
- Test specifications
- Protection profiles
- Test procedures

Security of payment procedures

- Credit
- Debit
- CBCDs

Know Your Customer (KYC)-procedures

- Expert groups
- Money laundering

Requiremtens for special methods of authentication

- Biometric
- Multi factor

(european) workinggroups

- Secure Element/eUICC
- Hardware-sicherheitsanker

Timeline

EU: DCC negotiations

Mar 2021

May 2021

Jan 2020

First covid case in Germany

Jun 2020

CWA published

CORONA WARN-APP

Feb 2021

Vaccination begins

June 2021

CovPass published

Timeline

Jan 2020
First covid case in Germany

Mar 2020
BSI: CWA participation

Jun 2020
CWA published

CORONA WARN-APP

Feb 2021
Vaccination begins

Mar 2021
EU: DCC negotiations

Spring 2021
BSI: CovPass participation

May 2021

June 2021
CovPass published

Corona-Warn-App (CWA)

Corona-Warn-App

- Developers: SAP & Telekom
- German App for Contact Tracing
- Pan-Eurpopean Privacy-Preserving Proximity Tracing (PEP-PT)
  vs.
  Decentralized Privacy-Preserving Proximity Tracing (DP^3T)
- Open source

CORONA
WARN-APP

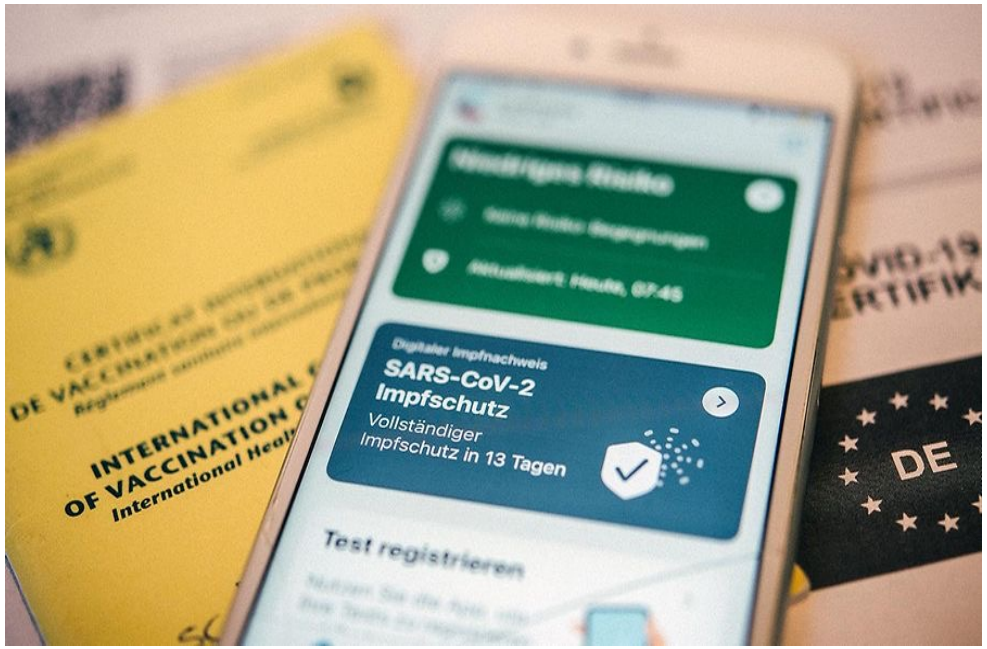
CovPass-App

Federal Office
for Information Security

ERNW
providing security.

CovPass-App

- Developer: IBM & Ubirch
- German app for Digital Covid Certificates (DCCs)
- EU-wide Public Key Infrastructure
- Dezentralized data storage



Federal Office
for Information Security

ERNW
providing security.

Assessments

Assessments

- Assignment via BMG/RKI
- Sprints
- 5- to 7-day pentest and code reviews (biweekly)
- White Box
  - Threat modelling workshops

What is special?

- Evolving subject
- Frequent and close collaboration with stakeholders
  - Periodic assessment
  - Weekly meetings
- Changing Requirements
- Process vs. product

Technical Approach

Assessment Approach per Iteration

Deployment	Diffing	Testing	Reporting

• Dedicated Testing Environment
• Testing-Apps
  • APK
  • TestFlight
• Source Code (GitHub and GitLab)
• Version info and commits
	• Source code diff between current and previous version
	• Mark interesting and important parts for later
	• Mark interesting and important parts based on changelog
		• Thorough assessment of new functionality (penetration test, source code audit, …)
		• Thorough assessment of parts marked in diffing phase
		• Automated and recurring tests (dependency scans, source code queries, …)
			• General rating and evaluation of the current state of the iteration
			• List and detailed description of all findings
			• Details about tested versions and covered commits

Assessment Approach per Iteration

Deployment

- Dedicated Testing Environment
- Testing-Apps
  - APK
  - TestFlight
- Source Code (GitHub and GitLab)
- Version info and commits

Diffing

- Source code diff between current and previous version
- Mark interesting and important parts for later
- Mark interesting and important parts based on changelog

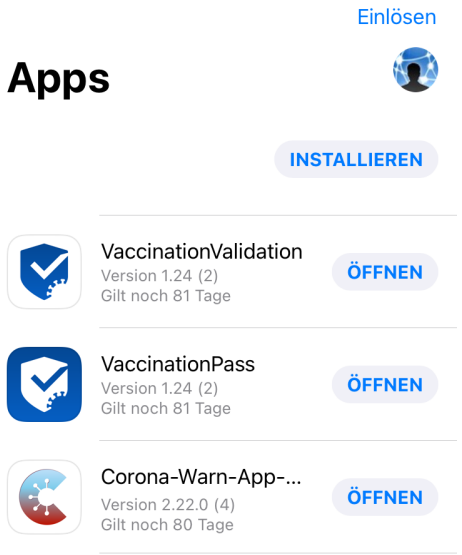
Testing

- Thorough assessment of new functionality (penetration test, source code audit, …)
- Thorough assessment of parts marked in diffing phase
- Automated and recurring tests (dependency scans, source code queries, …)

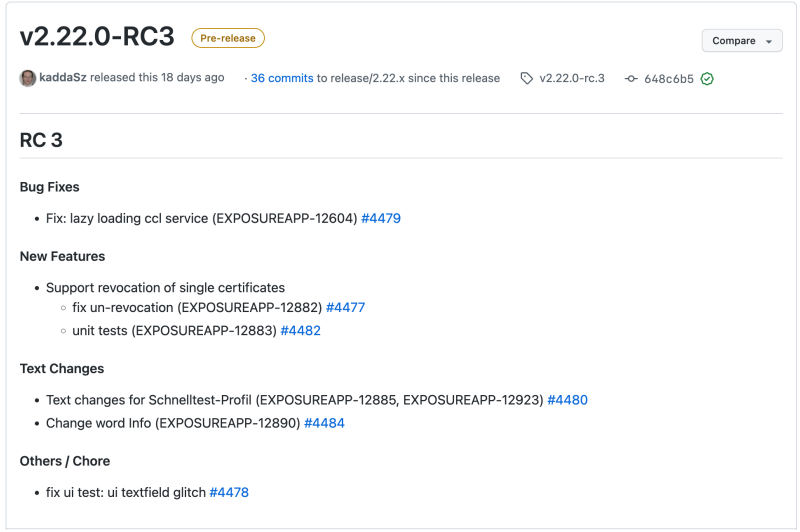
Reporting

- General rating and evaluation of the current state of the iteration
- List and detailed description of all findings
- Details about tested versions and covered commits

Assessment Approach: Deployment



iOS TestFlight deployment



v2.22.0-RC3

Pre-release

Compare

kaddaSz released this 18 days ago · 36 commits to release/2.22.x since this release · v2.22.0-rc.3 · 648c6b5

RC 3

Bug Fixes

- Fix: lazy loading ccl service (EXPOSUREAPP-12604) #4479

New Features

- Support revocation of single certificates
  - fix un-revocation (EXPOSUREAPP-12882) #4477
  - unit tests (EXPOSUREAPP-12883) #4482

Text Changes

- Text changes for Schnelltest-Profil (EXPOSUREAPP-12885, EXPOSUREAPP-12923) #4480
- Change word Info (EXPOSUREAPP-12890) #4484

Others / Chore

- fix ui test: ui textfield glitch #4478

Testgegenstand

Apps

Software-Modul	Repository	Version	Commit Hash	Funktions-Delta zur letzten Version	Art der Übergabe
Vaccination Certificate App (Android)		1.24	51aeabfdafc9f1d3af4f6979bcf5b516057c2b9e	~~BVC-4218~~ - [Android][CovPass] UI - Revoked certifcate superior detail screen - Wrong certifcate status logo/icon ~~BVC-4020~~ - [Android][CovPass] Wrong text for PCR tests in superior details page "Probenahme am ..." instead of "Getestet am ..." ~~BVC-3902~~ - [Android][CovPass]CovPass Refactoring – Adjust Value of JJ Vaccinations ~~BVC-3699~~ - [Android][CovPassCheck] - 2G+B - Different PI Screen is only shown if certificates are valid	
Vaccination App		1.24	51aeabfdafc9f1d3af4f6979bcf5b516057c2b9e	~~BVC-4219~~ - [Android][CovPassCheck] App crashes when process is cancelled in the loading screen	
on App		1.24(2)	328b134df40f5f00f0a365d0ad75188d91d4270b	~~BVC-4245~~ - [iOS][CovPass] Revocation - Error message is shown several times ~~BVC-3903~~ - [IOS][CovPass]CovPass Refactoring – Adjust Value of JJ Vaccinations	
on App		1.24(2)	328b134df40f5f00f0a365d0ad75188d91d4270b	~~BVC-3698~~ - [IOS][CovPassCheck] - 2G+B - Different PI Screen is only shown if certificates are valid ~~BVC-3818~~ - [iOS][CovPassCheck] 2G+ & 3G Wording in time designation	Testflight-Zugriff *Zugriff über den bestehenden Testflight-Account*

CovPass Iteration documentation

github.com/corona-warn-app/cwa-app-ios/releases/tag/v2.22.0-rc.3

Federal Office for Information Security

ERNW providing security.

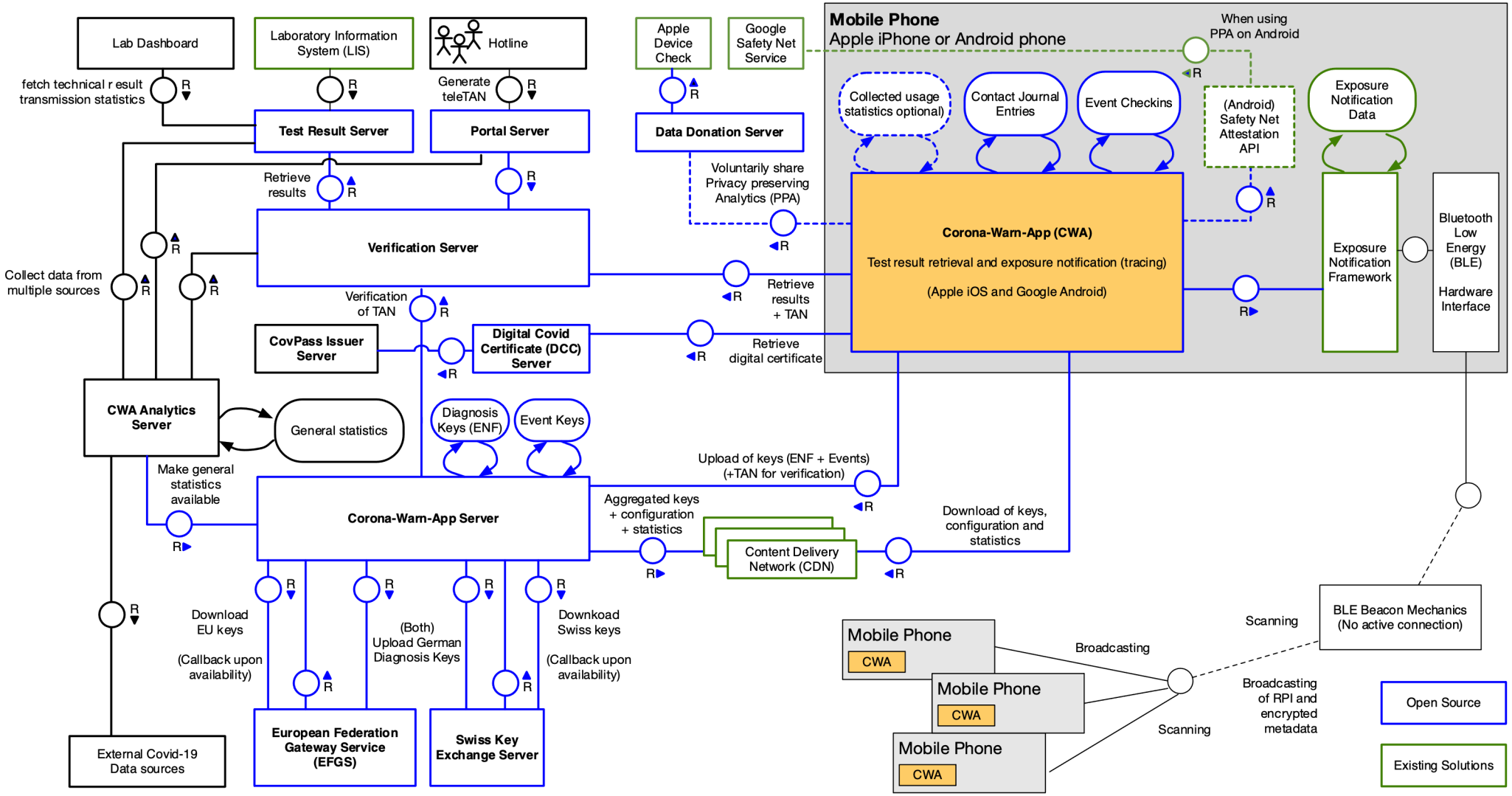
Components Covered

	Corona-Warn-App	CovPass
Mobile apps	2	4
Web interfaces	3	2
Backend systems	9	13
Total	**14**	**19**

On average. Some iterations require testing dedicated other components.

Federal Office for Information Security

ERNW providing security.



Federal Office for Information Security

ERNW providing security.

https://github.com/corona-warn-app/cwa-server/blob/main/docs/ARCHITECTURE.md

CovPass Backend Components

- Lots of microservices with separated responsibilities:
  - Vaccination Certificate Issuance
  - Signing Service
  - Point-of-Certification Management
  - Credential-Management Servers
  - Reissuance Servers

Programming Languages and Technologies

Corona-Warn-App	CovPass
Kubernetes	Kubernetes
Java	Scala Java Go Rust NodeJS
JavaScript / TypeScript / React	TypeScript / Angular
Swift Kotlin	Swift Kotlin

Excerpt, not a complete list of languages and technologies used.

Federal Office for Information Security

ERNW providing security.

Assessment Approach per Iteration

Deployment

- Dedicated Testing Environment
- Testing-Apps
  - APK
  - TestFlight
- Source Code (GitHub and GitLab)
- Version info and commits

Diffing

- Source code diff between current and previous version
- Mark interesting and important parts for later
- Mark interesting and important parts based on changelog

Testing

- Thorough assessment of new functionality (penetration test, source code audit, …)
- Thorough assessment of parts marked in diffing phase
- Automated and recurring tests (dependency scans, source code queries, …)

Reporting

- General rating and evaluation of the current state of the iteration
- List and detailed description of all findings
- Details about tested versions and covered commits

Assessment Approach: Diffing

Diffing also possible on GitHub:
github.com/corona-warn-app/cwa-app-ios/compare/v2.20.1...v2.21.1

- Diffing provides only little context
- Can only show what changed
- Challenge: what is important, what isn't (e.g., UI code)

33 src/xcode/ENA/ENA/Source/Extensions/TraceLocation+GenerateQRCode.swift

```
@@ -12,39 +12,8 @@ extension TraceLocation {
12                  guard let qrCodeURL = qrCodeURL else {
13                          return nil
14                  }
15 -
16 -                return qrCode(with: qrCodeURL, size: size, qrCodeErrorCorrectionLevel: qrCodeErrorCorrectionLevel)
17 -        }
18 -
19 -        // MARK: - Private
20 -
21 -        private func qrCode(with string: String, size: CGSize = CGSize(width: 400, height: 400),
   qrCodeErrorCorrectionLevel: MappedErrorCorrectionType = .medium) -> UIImage? {
22 -                /// Create data from string which will be feed into the CoreImage Filter
23 -                guard let data = string.data(using: .shiftJIS) else {
24 -                        return nil
25 -                }
26 -
27 -                /// Create CoreImage Filter to create QR-Code
28 -                guard let filter = CIFilter(name: "CIQRCodeGenerator") else {
29 -                        return nil
30 -                }
31 -                filter.setValue(data, forKey: "inputMessage") /// Feed data into Filter
32 -                filter.setValue(qrCodeErrorCorrectionLevel.mappedValue, forKey: "inputCorrectionLevel") /// Set
   ErrorCorrectionLevel
33 -
34 -                guard let image = filter.outputImage else {
35 -                        return nil
36 -                }
37 -
38 -                /// Depending on the length of the string the QRCode may vary in size. But we want an Image with a
   fixed size. This requires us to scale the QRCode to our desired image size.
39 -                /// Calculate scaling factors
40 -                let scaleX = size.width / image.extent.size.width
41 -                let scaleY = size.height / image.extent.size.height
42 -
43 -                /// Scale image
44 -                let transformedImage = image.transformed(by: CGAffineTransform(scaleX: scaleX, y: scaleY))
45
46 -                /// Return scaled image
47 -                return UIImage(ciImage: transformedImage)
48          }
49
50  }
```

```
@@ -12,39 +12,8 @@ extension TraceLocation {
12                  guard let qrCodeURL = qrCodeURL else {
13                          return nil
14                  }
15
16 +                return UIImage.qrCode(with: qrCodeURL, size: size, qrCodeErrorCorrectionLevel:
   qrCodeErrorCorrectionLevel)
17          }
18
19  }
```

Federal Office for Information Security

ERNW providing security.

Assessment Approach per Iteration

Deployment

- Dedicated Testing Environment
- Testing-Apps
  - APK
  - TestFlight
- Source Code (GitHub and GitLab)
- Version info and commits

Diffing

- Source code diff between current and previous version
- Mark interesting and important parts for later
- Mark interesting and important parts based on changelog

Testing

- Thorough assessment of new functionality (penetration test, source code audit, …)
- Thorough assessment of parts marked in diffing phase
- Automated and recurring tests (dependency scans, source code queries, …)

Reporting

- General rating and evaluation of the current state of the iteration
- List and detailed description of all findings
- Details about tested versions and covered commits

Assessment Approach per Iteration

Deployment

- Dedicated Testing Environment
- Testing-Apps
  - APK
  - TestFlight
- Source Code (GitHub and GitLab)
- Version info and commits

Diffing

- Source code diff between current and previous version
- Mark interesting and important parts for later
- Mark interesting and important parts based on changelog

Testing

- Thorough assessment of new functionality (penetration test, source code audit, …)
- Thorough assessment of parts marked in diffing phase
- Automated and recurring tests (dependency scans, source code queries, …)

Reporting

- General rating and evaluation of the current state of the iteration
- List and detailed description of all findings
- Details about tested versions and covered commits

Assessment Approach: Reporting

- About 80 reports in the last two years
- Lots of monotonic and recurring work → automate things!

```
auto-bsi iteration new --start 2022-06-13 --end 2022-06-15 v1.27

auto-bsi commits new ios-covpass abcd1234
auto-bsi commits diff
auto-bsi depscan scan

auto-bsi report finish
```

Assessment Approach: Reporting

The table below lists the status of the findings with regard to the previous report and potential changes:

Finding	Status
D[redacted]	Unchanged
In[redacted]	Unchanged
Z[redacted]	Unchanged
F[redacted]	Unchanged
U[redacted]	Unchanged
B[redacted]	Updated, new occurrence
Missing Input Validation	Fixed
Log Injection	Fixed
iOS Insufficient Escaping in vCard Construction	Fixed
Client-Side Controls	Fixed
Certificate Validity Manipulated by Phone Date and Time	Fixed

Table 3: Finding Status

3.1 Tested Versions

The following source code versions were covered during this test:

Component	Commit / Version	Notes
cwa-server	ff22458dde097435e1a2be1a1a0a85dcadcd8cef	
cwa-app-android	v2.13.0-RC1 - 0a7752da8ab88dc08419dfddf7a332	
cwa-app-ios	v2.13.0-RC4 - 241411170474cb05ff0b5e26350c8d	
cwa-verification-server	b793f63c19c6bf0cd4db3f486e05f2589456ab4f	
cwa-verification-portal	8e38494e2aeec7714306a8fa72cdefeb44a931b1	No changes since last iteration
cwa-verification-iam	81553106ad52771dfef0a3d51d057a905365d9d9	No changes since last iteration
cwa-testresult-server	ac78a0c2f9d85243eac69916fb1938d758dff80e	
cwa-ppa-server	bb5e888379e3e5cb28bcf677434bb446b49f29cc	
cwa-log-upload	9ef47b7104bd5128848a6e986ff4cae5cbe574ee	No changes since last iteration
cwa-quick-test-frontend	6ee84402c858b86d1a2055e327a051079c8b47ed	
cwa-quick-test-backend	ec8af1c458d264fb74adcb89924e800050e06e3e	No changes since last iteration
Corona Warn App Analytics	bfc649beb9252018abd9700130afdc57576b77f1	
cwa-dcc-server	41270069243f7c5da50a2a22df15b157f425a809	No changes since last iteration
dgca-businessrule-service	ec0326d8dd72f220c4b8e0e54e285869b0d3e730	No changes since last iteration

Table 6: Overview of Tested Versions

The following release candidate app versions were provided for the Test:

- iOS App Version 2.13.0 RC1
- Android App Version 2.13.0 RC4

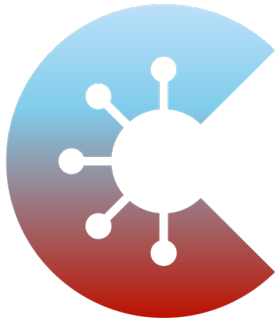
Federal Office for Information Security

ERNW providing security.

Vulnerability Examples

CWA iOS: SQL Injection

- During downloading and storing keys from the server
- Found and mitigated prior to the public release of the app version
- Publicly documented on GitHub https://github.com/corona-warn-app/cwa-app-ios/issues/1533



CORONA
WARN-APP

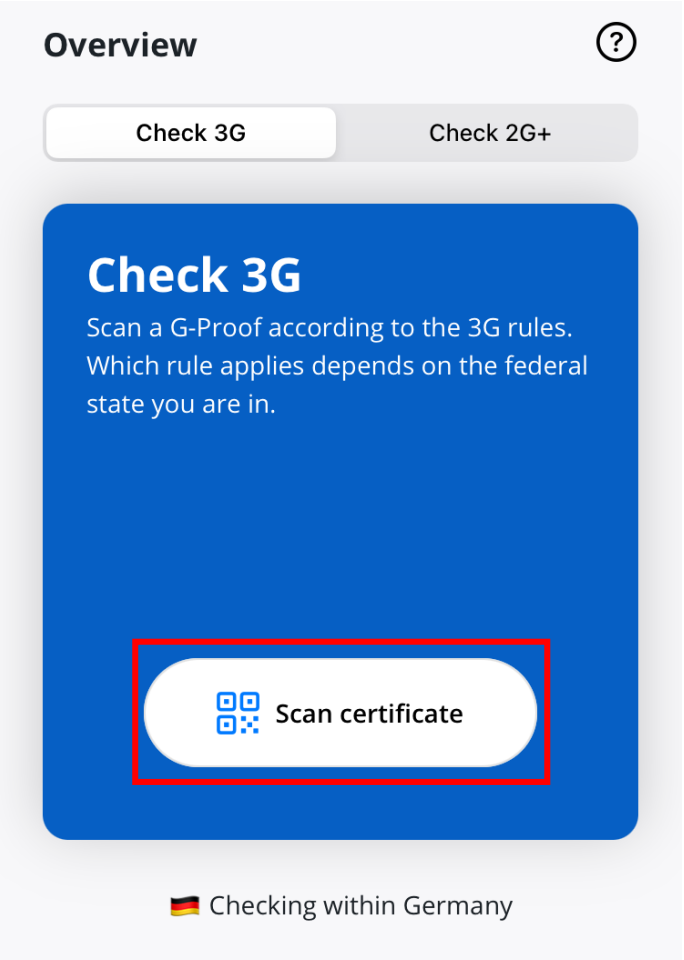
etags array originates from server

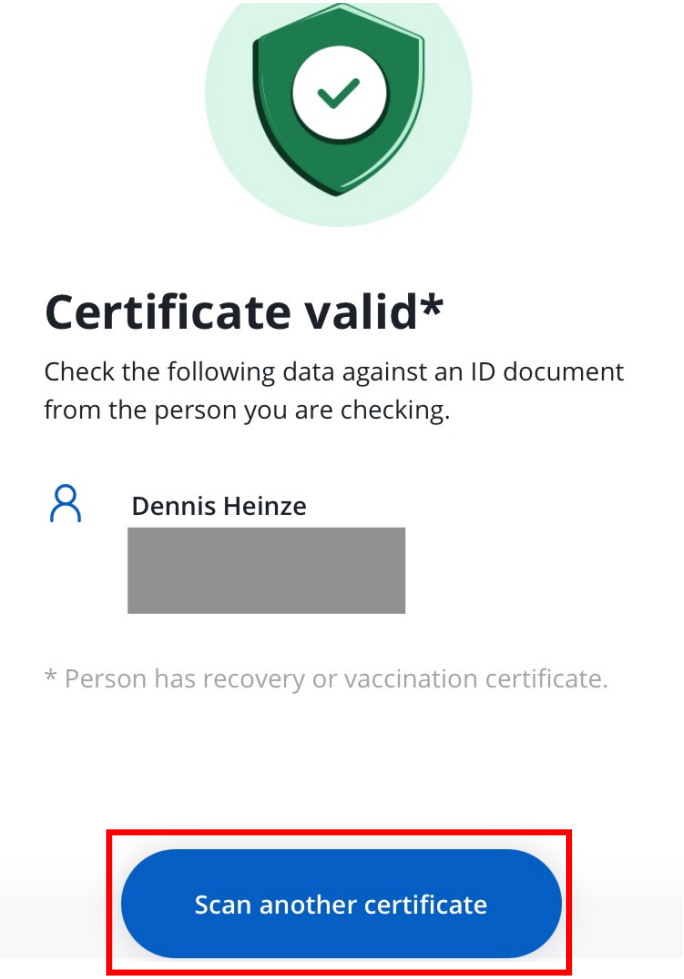
```
queue.sync {
    let list = "(\(etags.map({ "\'\($0)\'" }).joined(separator: ",")))" // ('a','b','c')
    let sql = """
        SELECT
            Z_BIN,
            Z_SIGNATURE
        FROM Z_DOWNLOADED_PACKAGE
        WHERE
            Z_ETAG
        IN
            \(list)
        ;
    """
    let parameters: [String: Any] = [:]
    guard let result = self.database.execute(query: sql, parameters: parameters) else {
```

Will be placed in SQL query string

CovPassCheck iOS: Logic Bug

- Missing validation of the certificate after tapping “scan another certificate”
- Found and mitigated prior to the public release of the app version


Overview
Check 3G
Check 2G+
Check 3G
Scan a G-Proof according to the 3G rules. Which rule applies depends on the federal state you are in.
Scan certificate
Checking within Germany


Certificate valid*
Check the following data against an ID document from the person you are checking.
Dennis Heinze
* Person has recovery or vaccination certificate.
Scan another certificate

First Scan

```
func startQRCodeValidation() {
    firstly {
        router.scanQRCode()
    }
    .map {
        try self.payloadFromScannerResult($0)
    }
    .then {
        self.process(payload: $0)
    }

    […]
}


func process(payload: String) -> Promise<CBORWebToken> {
    repository.checkVaccinationCertificate(payload)
}
```

Certificate is validated

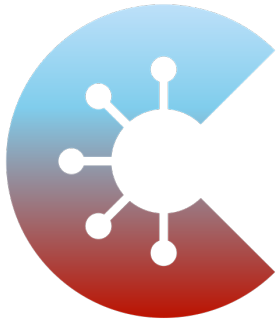
Next Scan

```
func scanNextCertifcate() {
    firstly {
        router.scanQRCode()
    }
    .map {
        try self.payloadFromScannerResult($0)
    }
    .then {
        self.process(payload: $0)
    }

    […]
}


private func process(payload: String) -> Promise<CBORWebToken> {
    return parser.parse(payload)
}
```

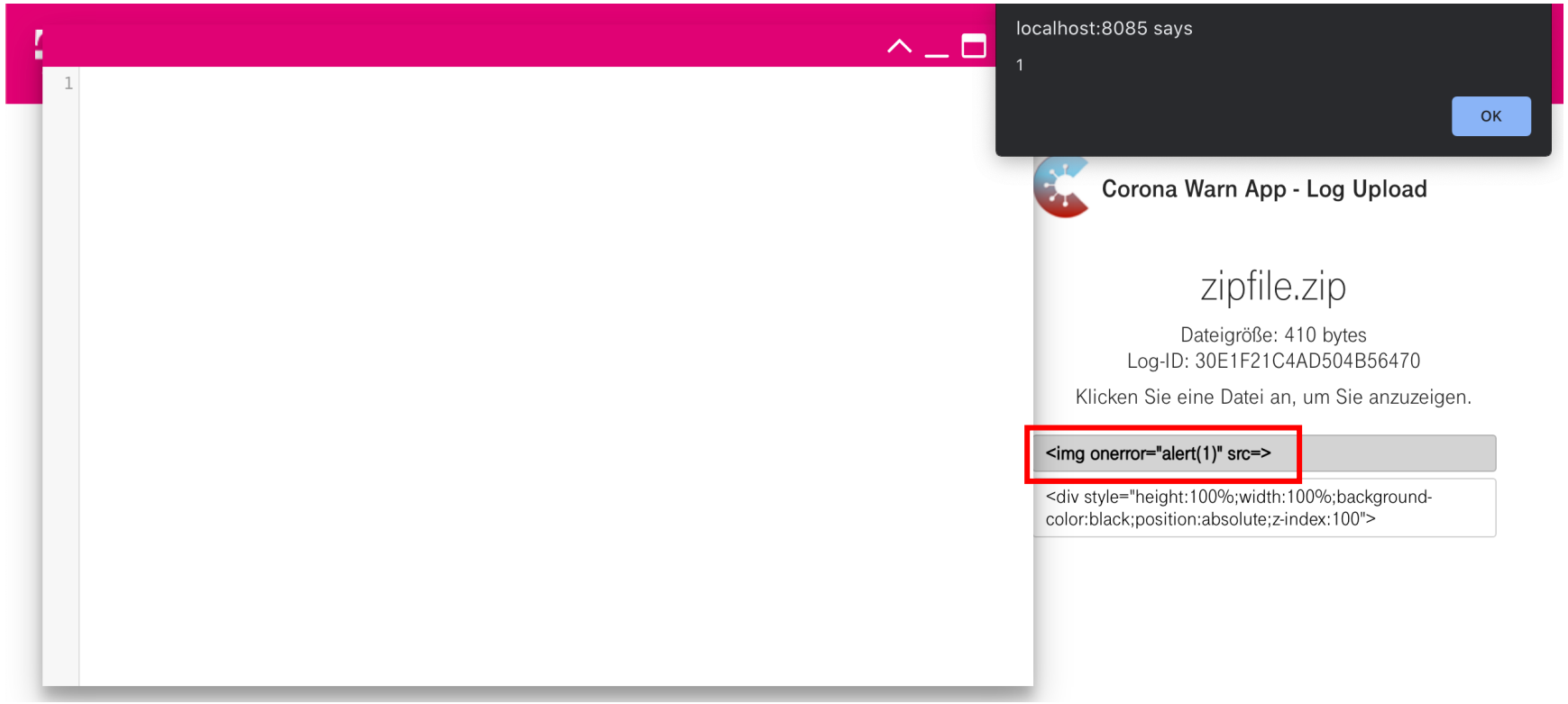
Certificate is only parsed

CWA Backend: Log Upload XSS

- The mobile apps allow uploading logs in case of errors
- This logfile (ZIP archive) can be downloaded by developers
- Stored XSS in the uploaded file



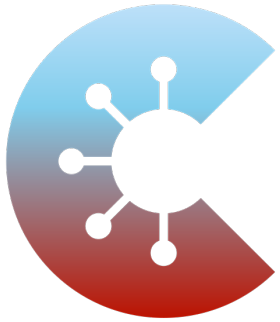
CORONA
WARN-APP


localhost:8085 says
1
OK
Corona Warn App - Log Upload
zipfile.zip
Dateigröße: 410 bytes
Log-ID: 30E1F21C4AD504B56470
Klicken Sie eine Datei an, um Sie anzuzeigen.
<img onerror="alert(1)" src=>

1

CWA Backend: Log Upload XSS

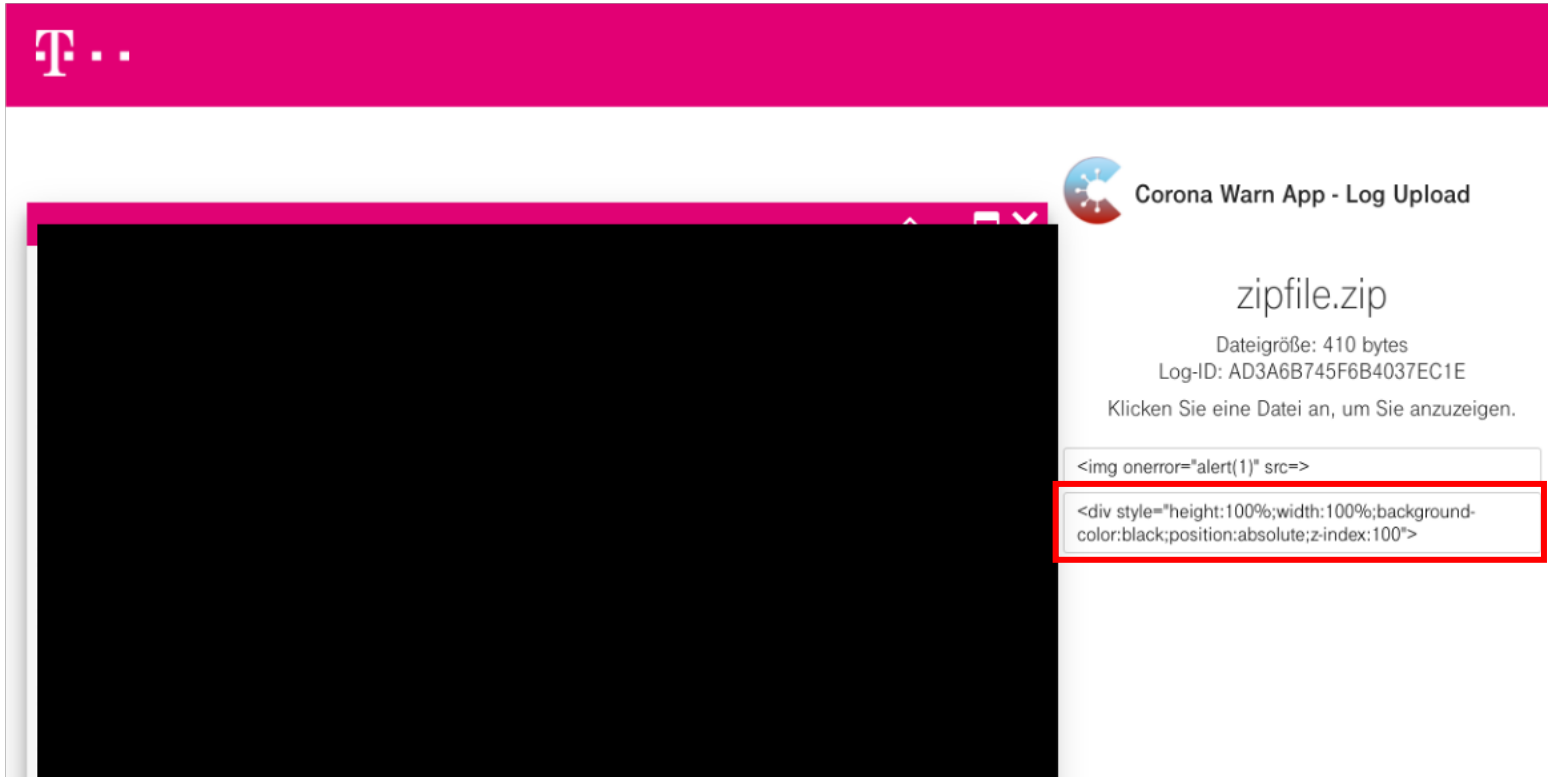
- First fix incomplete
- No XSS but still allowed HTML injection (violates integrity of the page)



CORONA
WARN-APP

Federal Office
for Information Security

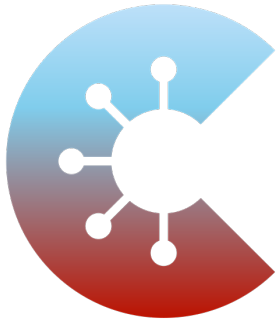
ERNW
providing security.


Corona Warn App - Log Upload
zipfile.zip
Dateigröße: 410 bytes
Log-ID: AD3A6B745F6B4037EC1E
Klicken Sie eine Datei an, um Sie anzuzeigen.
<img onerror="alert(1)" src=>

[redacted]

CWA Backend: Log Upload XSS

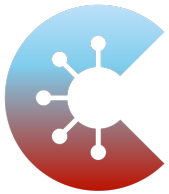
- First fix incomplete
- No XSS but still allowed HTML injection (violates integrity of the page)
- Lastly it was refactored to completely rule out the issue (filename is not displayed at all)



CORONA
WARN-APP

Both: Log Injection

- Violate integrity of server logs
- Interesting bug class especially for CovPass audit logging (*who issued which certificate*)



CORONA
WARN-APP

```
7.197  INFO [cwa-log-upload,,] 50977 --- [           main] o.s.s.c.ThreadPoolTaskScheduler          : Initializing ExecutorService 'taskSchedul
7.435  INFO [cwa-log-upload,,] 50977 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8085 (http) wi
7.480  INFO [cwa-log-upload,,] 50977 --- [           main] a.c.logupload.LogUploadApplication       : Started LogUploadApplication in 18.849 se
3.743  INFO [cwa-log-upload,,] 50977 --- [nio-8085-exec-1] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring DispatcherServlet 'di
3.744  INFO [cwa-log-upload,,] 50977 --- [nio-8085-exec-1] o.s.web.servlet.DispatcherServlet        : Initializing Servlet 'dispatcherServlet'
3.746  INFO [cwa-log-upload,,] 50977 --- [nio-8085-exec-1] o.s.web.servlet.DispatcherServlet        : Completed initialization in 2 ms
3.830  INFO [cwa-log-upload,a2d8263b1fc90155,a2d8263b1fc90155] 50977 --- [nio-8085-exec-1] a.c.l.controller.LogUploadApiController  : Got file:
3.831  INFO [cwa-log-upload,a2d8263b1fc90155,a2d8263b1fc90155] 50977 --- [nio-8085-exec-1] a.c.l.service.FileStorageService         : Persistir
4.085  INFO [cwa-log-upload,a2d8263b1fc90155,a2d8263b1fc90155] 50977 --- [nio-8085-exec-1] a.c.l.service.FileStorageService         : File stor

4.086  INFO [cwa-log-upload,a2d8263b1fc90155,a2d8263b1fc90155] 50977 --- [nio-8085-exec-1] a.c.l.service.FileStorageService         : Storing L
4.138  INFO [cwa-log-upload,a2d8263b1fc90155,a2d8263b1fc90155] 50977 --- [nio-8085-exec-1] a.c.l.controller.LogUploadApiController  : Saved log

9.583  INFO [cwa-log-upload,95191bcbb322938b,95191bcbb322938b] 50977 --- [nio-8085-exec-2] a.c.l.controller.LogUploadApiController  : Got file:
9.583  INFO [cwa-log-upload,95191bcbb322938b,95191bcbb322938b] 50977 --- [nio-8085-exec-2] a.c.l.service.FileStorageService         : Persistir
9.594  INFO [cwa-log-upload,95191bcbb322938b,95191bcbb322938b] 50977 --- [nio-8085-exec-2] a.c.l.service.FileStorageService         : File stor

9.594  INFO [cwa-log-upload,95191bcbb322938b,95191bcbb322938b] 50977 --- [nio-8085-exec-2] a.c.l.service.FileStorageService         : Storing L
9.597  INFO [cwa-log-upload,95191bcbb322938b,95191bcbb322938b] 50977 --- [nio-8085-exec-2] a.c.l.controller.LogUploadApiController  : Saved log

3.267  INFO [cwa-log-upload,f9f8cee82823c182,f9f8cee82823c182] 50977 --- [nio-8085-exec-3] a.c.l.controller.LogUploadApiController  : Got file:
7.277  INFO [cwa-log-upload,,] 50287 --- [           main] a.c.logupload.LogUploadApplication       : Injected Log Line, 458
3.267  INFO [cwa-log-upload,f9f8cee82823c182,f9f8cee82823c182] 50977 --- [nio-8085-exec-3] a.c.l.service.FileStorageService         : Persistir
3.278  INFO [cwa-log-upload,f9f8cee82823c182,f9f8cee82823c182] 50977 --- [nio-8085-exec-3] a.c.l.service.FileStorageService         : File stor

3.278  INFO [cwa-log-upload,f9f8cee82823c182,f9f8cee82823c182] 50977 --- [nio-8085-exec-3] a.c.l.service.FileStorageService         : Storing L
3.281  INFO [cwa-log-upload,f9f8cee82823c182,f9f8cee82823c182] 50977 --- [nio-8085-exec-3] a.c.l.controller.LogUploadApiController  : Saved log
```

Federal Office for Information Security

ERNW providing security.

Vulnerabilities in Third Party Components

- Third party components are not explicitly in scope
- However during testing we came across multiple vulnerabilities in different types of third party components
- These were communicated to BSI which initiated a CVD (coordinated vulnerability disclosure) with the vendor

Vulnerabilities in Third Party Components

- Examples
  - Local privilege escalation via exploitation of an SUID binary
  - DoS in parsing library
  - RCE, SQLi and partial authentication bypass in server component
  - RCE in client software

Conclusion

Conclusion

- Very good state of security on both projects (despite difficult circumstances)
- Testing is sometimes hard:
  - Changing requirements
  - Short timeframes for testing
  - Unexpected changes in schedule or implementation
- Developers are supportive
- Also: don’t underestimate third party components!

Conclusion

- Very good state of security on both projects (despite difficult circumstances)
- Testing is sometimes hard:
  - Changing requirements
  - Short timeframes for testing
  - Unexpected changes in schedule or implementation
- Developers are supportive
- Also: don’t underestimate third party components!

- Digitalization must consider security aspects – also in volatile projects
- Security begins by design
- In-house reviews and pentests must be performed
- External reviews/examinations help (certification)

Federal Office for Information Security

ERNW providing security.

Guiding principle

BSI as the Federal Cyber Security Authority shapes information security in digitalization through prevention, detection and response for government, business and society.

Thank you for your attention!

Deutschland
Digital•Sicher•BSI•

Contact Details

Pascal Jeschke
Cyber Security for Digitalisation in the Public Health and the Financial Services Sector
Tel.: +49 228 99 9582-4160
Mail: pascal.jeschke@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Dennis Heinze
Security Analyst & Researcher
Mail: dheinze@ernw.de

Federal Office for Information Security

ERNW providing security.