Von: [redacted] BMG
An: [redacted]
Betreff: WG: Pentest BSI SORMAS
Datum: Mittwoch, 2. Dezember 2020 19:09:12

Lieber [redacted],

wir haben uns nach dem Pen-Test noch garnicht wieder ausgetauscht. Daher auch noch einmal ein ausdrückliches Dankeschön von unserer Seite für die Prüfung und die wichtigen Hinweise.

Ungern schließe ich an eine solche Danksagung direkt eine Bitte an, jedoch würde ich mich freuen, wenn wir uns in den kommenden Tagen einmal zu etwaigen Möglichkeiten eines Re-Tests der Anwendungen hinsichtlich der Behebung der Mängel austauschen könnten.

Ich bedanke mich vorab vielmals und wünsche Ihnen noch einen angenehmen Abend

Viele Grüße
[redacted]

-----Ursprüngliche Nachricht-----
Von: [redacted]
Gesendet: Mittwoch, 2. Dezember 2020 17:57
An: [redacted]@bsi.bund.de>; [redacted]
Cc: [redacted]@bmg.bund.de>; [redacted]
[redacted]@bsi.bund.de>; [redacted]
Betreff: Re: Pentest BSI SORMAS

Hallo [redacted]

gerne informiere ich Sie heute über den Status der Arbeiten an Ihren Findings aus dem Pen-Test.

Von Ihren 12 Findings sind aktuell
- 1 Ticket zur Information
- 3 bei [redacted] in Arbeit (5.1.1, 5.1.2, 5.1.3). Diese werden mit dem nächsten Rollout behoben sein.
- 8 konnten wir bei der [redacted] adressieren
- 5.2.1 ist im Produktivsystem natürlich kein issue mehr
- 5.2.2 ist durch die Integration von Keycloak abgegolten (https://github.com/hzi-braunschweig/SORMAS-Project/issues/2745)
- 5.2.3 kann entsprechend besser mit keycloak konfiguriert werden (flexible Password-Policy Einstellungen)
- 5.2.4 ist bereits gelöst und in der Version 1.50 gefixed worden (https://github.com/hzi-braunschweig/SORMAS-Project/issues/2745)
- 5.3.1 ist bereits gelöst und in der Version 1.51 gefixed worden (https://github.com/hzi-braunschweig/SORMAS-Project/issues/2990)
- 5.3.2 resultierte in mehreren Issues und ist mit der 1.50.0 gelöst worden
https://github.com/hzi-braunschweig/SORMAS-Project/issues/2859
https://github.com/hzi-braunschweig/SORMAS-Project/pull/3083
https://github.com/hzi-braunschweig/SORMAS-Project/issues/2991
https://github.com/hzi-braunschweig/SORMAS-Project/pull/3118
- 5.3.3 ist gerade in Arbeit und wird mit der 1.53.0 die für Mitte Dezember geplant ist, gelöst werden (https://github.com/hzi-braunschweig/SORMAS-Project/issues/3578)
- 5.4.1 ist unserer Ansicht nach kein Issue, da es sich um ein Open Source Projekt handelt und ohnehin jeder auf den Code zugreifen kann. Ich habe aber [redacted] informiert, dass er das nochmals prüfen soll
- 5.5.1 ist in Arbeit und wird mit der 1.53.0 die für Mitte Dezember geplant ist, gelöst werden (https://github.com/hzi-braunschweig/SORMAS-Project/issues/3584)

Ich habe Ihnen einen pdf-Export unserer Confluence-Seite angehängt, wo wir den Status dokumentieren.

Viele Grüße und einen schönen Abend,

[redacted]

Am 21.10.20, 10:56 schrieb [redacted]@bsi.bund.de>:

Sehr geehrter [redacted]

ich bin der koordinierende Penetrations-Tester, der im BSI mit den SORMAS-Tests betraut wurde.
Sie wurden mir als Ansprechpartner der [redacted] genannt.
Ich wurde von der [redacted] darauf hingewiesen, dass es vor den anstehenden Penetrationstests von SORMAS die Datenbank bereinigt und die neuste Version von SORMAS installiert werden soll (siehe unten stehende Mail).
Dies soll von der [redacted] durchgeführt werden.
Die Penetrationstests sollen am 26.10.2020 beginnen und zwei Wochen andauern.
Können Sie mir hier weiterhelfen?

Vielen Dank im Voraus.

Freundliche Grüße,
Im Auftrag,

[redacted]

Referat DI 24 - Cyber-Sicherheit im Gesundheits- und Finanzwesen
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Telefon: +49 (0)228 99 9582-[redacted]
Fax: +49 (0)228 99 10 9582[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de

Besucheradresse: Heinemannstraße 11-13, 53175 Bonn

-----Ursprüngliche Nachricht-----
Von: [redacted]
Gesendet: Mittwoch, 21. Oktober 2020 08:39
An: [redacted]@bsi.bund.de>;
Cc: [redacted]@bmg.bund.de; GP Referat DI 24 <referat-di24@bsi.bund.de>; [redacted]@bsi.bund.de>
Betreff: Re: Pentest BSI SORMAS

Sehr geehrter [redacted],

gerne stelle ich Ihnen die Informationen zu unserem bisherigen Penetrationstest bereit.
Jedoch sollte vor der Überprüfung durch das BSI die Datenbanken bereinigt und die neuste Version von SORMAS auf den Systemen installiert werden.
Hier kann die [redacted] unterstützen.

- URL zum Frontend:
[redacted]

- API Docs (z.B. Swagger, Postman, o. Ä.) zum Backend:
Die Dokumentation ist in unserem Git Repository vorhanden.

- URL zum git Repository:
https://github.com/hzi-braunschweig/SORMAS-Project

- User Accounts (falls nicht selbst erstellbar):
Für den Login wurden die bei der Installation standardmäßig erstellten Benutzer verwendet.
Zu finden sind diese unter: [redacted]

- Docker Container (falls möglich):
Zur lokalen Installation kann das Git Repository verwendet werden.
Für eine Konfigurationsprüfung wird ein VPN-Zugang benötigt, welchen die [redacted] bereitstellt.

Viele Grüße,

[redacted]

Am 20.10.20, 15:19 schrieb "[redacted]

Sehr geehrter [redacted],

leider habe ich von diesen technischen Dingen in der Tiefe nur sehr begrenzt Ahnung. Ihr passender Ansprechpartner ist [redacted] (siehe cc), der Ihnen die entsprechenden Informationen zukommen lassen wird.

Viele Grüße
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

--

Bitte beachten Sie unsere Hinweise zur Datenverarbeitung.

-----Ursprüngliche Nachricht-----
Von: [redacted]@bsi.bund.de>
Gesendet: Dienstag, 20. Oktober 2020 15:14
An: [redacted]
Cc: [redacted]@bmg.bund.de; GP Referat DI 24 <referat-di24@bsi.bund.de>; [redacted]@bsi.bund.de>
Betreff: Pentest BSI SORMAS

Sehr geehrter [redacted]

ich bin der koordinierende Penetrations-Tester, der im BSI mit den SORMAS-Tests betraut wurde.
Sie wurden mir als Ansprechpartner für die SORMAS-Tests genannt.
Um die BSI-Pentests in den kommenden Wochen möglichst effizient durchführen zu können, würde ich Sie um folgende Informationen bitten:

- URL zum Frontend
- API Docs (z.B. Swagger, Postman, o. Ä.) zum Backend
- URL zum git Repository
- User Accounts (falls nicht selbst erstellbar)
- Docker Container (falls möglich)

Vielen Dank im Voraus für Ihre Hilfe.

Freundliche Grüße,
Im Auftrag,

[redacted]

Referat DI 24 - Cyber-Sicherheit im Gesundheits- und Finanzwesen Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Telefon: +49 (0)228 99 9582-[redacted]
Fax: +49 (0)228 99 10 9582[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de

Besucheradresse: Heinemannstraße 11-13, 53175 Bonn