Joachim Lindenberg

Von: CERT-Bund <certbund@bsi.bund.de>
Gesendet: Tuesday, 15 February 2022 07:13
An: [redacted]@lindenberg.one
Betreff: [CERT-Bund#2022020828000621] Ihre Meldung an das CERT-Bund
Anlagen: pgp_sign.asc

Sehr geehrter Herr Lindenberg,

vielen Dank für Ihre Meldung an das Bundesamt für Sicherheit in der Informationstechnik (BSI). Nach eingehender Prüfung Ihrer Meldung werden wir kein CVD-Verfahren einleiten, da es sich bei dem vorliegenden Sachverhalt nicht um eine Schwachstelle handelt. Vielmehr können Ihre Funde als fehlende Umsetzung von Best Practices bezeichnet werden.

Es wird deshalb kein CVD-Verfahren eingeleitet und keine weiteren Schritte veranlasst.

Mit freundlichen Grüßen
das Team CERT-Bund

--
Bundesamt für Sicherheit in der Informationstechnik (BSI)
CERT-Bund
Godesberger Allee 185-189
D-53175 Bonn
Web: https://www.bsi.bund.de/CERT-Bund/
PGP & S/MIME: https://www.bsi.bund.de/CERT-Bund-Kontakt

#DeutschlandDigitalSicherBSI

Alle Informationen zum Umgang mit Ihren personenbezogenen Daten finden Sie unter www.bsi.bund.de/datenschutz

Am 08.02.2022 07:24 wrote CERT-Bund:
##################################
Dies ist eine automatisch erstellte Mail
##################################

Sehr geehrte Damen und Herren,

vielen Dank für Ihre Schwachstellenmeldung an das Bundesamt für Sicherheit in der Informationstechnik (BSI), deren Erhalt wir hiermit bestätigen.

Wir werden Ihre Schwachstellenmeldung und die dazugehörigen Informationen zeitnah prüfen und uns anschließend mit Ihnen in Verbindung setzen, um das weitere Vorgehen zu besprechen.
Sollten Ihrerseits Rückfragen entstehen, können Sie sich jederzeit über die im Betreff angegebene Ticketnummer CERT-Bund#2022020828000621 an uns wenden.
Wir bitten um Verständnis, dass ein mehrfaches Melden derselben gefundenen Schwachstelle keine höhere Priorisierung dieser bewirkt.

Bitte beachten Sie für den Fall, dass Sie personenbezogene Daten in der Meldung oder im Meldeformular angegeben haben die Hinweise des BSI zum Datenschutz:
https://www.bsi.bund.de/DE/Service/Datenschutz/datenschutz_node.html
Hinweise zu Meldestellen sind insbesondere in Ziffer 10 enthalten. Sollten Sie als Ansprechpartner keine Funktions- oder Organisationseinheit angegeben haben/können bzw. als Kontaktadresse über kein Funktionspostfach verfügen, setzen Sie bitte den in der Meldung genannten Ansprechpartner über die oben genannten Datenschutzhinweise in Kenntnis.

Mit freundlichen Grüßen
CERT-Bund

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
D-53175 Bonn

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Schwachstellenmeldung **Onlineformular für Schwachstellen**

An das BSI gemeldete Schwachstellen und Sicherheitslücken in IT-Produkten oder IT-Diensten werden in der Regel in Anlehnung an die **ISO-Norm 29147** im „Coordinated Vulnerability Disclosure (CVD)" - Verfahren an den Hersteller des Produktes bzw. den Dienstleister weitergeleitet. Fallbezogen kann das BSI zudem während des anschließenden Behebungsprozesses als Koordinator unterstützend tätig werden.
Die Meldung kann auf Wunsch auch anonymisiert erfolgen. Bitte beachten Sie in diesem Fall möglichst umfassende und präzise Angaben zu machen, die eine Verifikation und Bewertung des Sachverhalts ermöglichen, da Rückfragen durch das BSI in diesem Fall nicht möglich sind.
Als Meldender bestimmen Sie darüber, inwieweit Ihre Beteiligung dem Hersteller gegenüber offengelegt wird. Nutzen Sie hierfür insbesondere die letzten Eingabefelder des Formulars.

Bitte kopieren Sie keinen Quellcode in die Textfelder, da unsere Sicherheitsmechanismen die Übertragung solcher Inhalte verhindern. Die Meldung wird geblockt und nicht an uns verschickt. Verwenden Sie bitte auch keine Anführungszeichen.

Zweck der Meldung * (Pflichtangabe)

Mit der Bitte um Übernahme, Einleitung und Koordinierung des Coordinatec

Details zur Schwachstelle / Sicherheitslücke

Haben Sie bereits versucht den Hersteller des Produkts oder den Betreiber des Online-Dienst kontaktieren? * (Pflichtangabe)

Nein

Name des Herstellers des Produkts oder des Betreibers des Online-Dienstes? * (Pflichtangabe)

Sieh Text

Sind nach Ihrem Kenntnisstand mehrere Hersteller oder Betreiber betroffen? * (Pflichtangabe)

Ja

Um welches Produkt oder welchen Online-Dienst handelt es sich? * (Pflichtangabe)

Email von Behörden und Anwälten, vermutlich viele weitere Anbieter/Betreiber

Welche Version wurde von Ihnen getestet?
(Konkretisierende Hinweise zur Versionsbezeichnung, Firmware Version, Build Nummer oder Veröffentlichungsdatum, um eine Eingrenzung zu erleichtern. Soweit dies für Sie nicht ersichtlich war, tragen Sie bitte „unbekannt" ein.) *** (Pflichtangabe)**

unbekannt

Um welche Schwachstelle oder Sicherheitslücke handelt es sich?
(Bitte beschreiben Sie das Problem in ausreichender technischer Detailtiefe. Soweit es Ihnen möglich ist, geben Sie ein reproduzierbares Beispiel an bzw. einen Proof-of-Concept. Sie können hier mehrere Sachverhalte zum selben Produkt oder Online-Dienst zusammenfassen. Es stehen Ihnen 20.000 Zeichen zur Verfügung.) *** (Pflichtangabe)**

Fehlende Untersützung von RFC 7672 SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS). Die Angriffsvektoren sind in Abschnitt 1.3 beschrieben.

Wie kann ein Angreifer die Schwachstelle oder Sicherheitslücke ausnutzen?
(Bitte beschreiben Sie die Ihnen bekannten Rahmenbedingungen, unter denen dies erfolgen muss. Es stehen Ihnen 20.000 Zeichen zur Verfügung.) *** (Pflichtangabe)**

Siehe Abschnitt 1.3 des genannten RFCs.

Was kann der Angreifer durch die Ausnutzung der Schwachstelle oder der Sicherheitslücke erreichen?
(Welche spezifischen Auswirkungen, welchen Impact erzielt der Angreifer durch die zuvor beschriebene Ausnutzung der Schwachstelle? Es stehen Ihnen 20.000 Zeichen zur Verfügung.) *** (Pflichtangabe)**

Siehe Abschnitt 1.3 des genannten RFCs.

Wie wurde die Schwachstelle bzw. die Sicherheitslücke entdeckt?
(Haben Sie spezielle Tools oder Methoden verwendet? Es stehen Ihnen 20.000 Zeichen zur Verfü
(Pflichtangabe)

Siehe https://blog.lindenberg.one/EmailsicherheitOffentlicheEinrichtungen und https://blog.lindenberg.one/EmailsicherheitAnwalte. Von den untersuchten ca 45.000 Domänen sind nur ca 1.600 geschützt, die anderen rund 43.000 sind angreifbar.

Ist die Schwachstelle bzw. die Sicherheitslücke nach Ihrem Kenntnisstand bereits öffentlich bekannt? ***(Beispielsweise auch in Foren oder Blogs.)*** *** (Pflichtangabe)**

Ja

Wird die Schwachstelle bzw. die Sicherheitslücke nach Ihrem Kenntnisstand bereits aktiv ausgenutzt? * (Pflichtangabe)

Unbekannt

Beabsichtigen Sie die Schwachstelle bzw. die Sicherheitslücke selbst öffentlich bekannt zu machen? * (Pflichtangabe)

Ja

Persönliche Kontaktinformationen

Name
(Optionale Angabe. Die Meldung kann sowohl anonym als auch unter Verwendung eines Pseudonyms erfolgen, sofern Sie die Möglichkeit für eine spätere Kommunikation aufrecht erhalten möchten.)

Joachim Lindenberg

Organisation
(Optionale Angabe. Bitte benennen Sie die Organisation, soweit Sie in deren Auftrag handeln.)

E-Mail-Adresse
(Optionale Angabe. Bitte ziehen Sie die Nutzung eines kostenlosen Webmail-Anbieters, zur einmaligen Nutzung für diese Meldung in Betracht, sofern Sie Ihre persönliche Mail-Adresse nicht mitteilen wollen.)

[redacted]@lindenberg.one

Telefon
(Optionale Angabe, um kurzfristig direkte Rückfragen zu ermöglichen.)

Öffentlicher PGP Schlüssel
(Optionale Angabe. Es empfiehlt sich, vertrauliche Informationen zu verschlüsseln. Bitte fügen Sie hier Ihren öffentlichen (ASCII armored) PGP Key oder eine URL zu diesem ein.)

Wünschen Sie eine Weitergabe Ihrer Kontaktdaten an den Hersteller?
(Sofern nicht explizit von Ihnen gewünscht, werden Ihre Kontaktdaten nicht an den Hersteller weitergegeben.)

Nein

Wünschen Sie in Veröffentlichungen bzw. Warnungen zu dieser Schwachstelle bzw. Sicherheitslücke namentlich genannt zu werden?
(Sofern nicht explizit von Ihnen gewünscht, werden Sie nicht standardmäßig namentlich genannt werden.)

Ja

Ihre privaten Anmerkungen
(Optionale Angabe. Anmerkungen, Details oder sonstige Absprachen, die Sie hier in diesem Feld eintragen werden nicht ohne Ihre explizite, vorherige Zustimmung in eine Veröffentlichung bzw. Warnung mit aufgenommen oder mit dem Hersteller geteilt.)

Die Schwachstelle ist ja nicht neu, RFC 7672 ist gut sechs Jahre alt. Was fehlt ist eine klare Erwartung der Behörden und der Aufsicht, diesen RFC umzusetzen. Weder das BSI noch das BfDI erwähnt diesen RFC. Auch ist PGP oder S/MIME m.E. keine Alternative, denn auch Kommunikationsmetadaten unterliegen dem Fernmeldegeheimnis und dem Datenschutz, diese

CERT-Bund Ticket ID
(Optionale Angabe. Sofern Sie bezüglich dieses Vorgangs bereits mit CERT-Bund in Kontakt standen und eine Ticket ID vergeben wurde, geben sie diese hier bitte an.)

Bitte geben Sie die Buchstaben aus dem CAPTCHA-Feld ein. * (Pflichtangabe)

turters

Ich willige in die Verarbeitung meiner personenbezogenen Daten zum Zwecke der Kontaktaufnahme gem. Artikel 6 Absatz 1 lit a Datenschutzgrundverordnung (DSGVO) ein. Nach Artikel 13 der Datenschutzgrundverordnung (DSGVO) möchten wir Sie über die Verarbeitung Ihrer personenbezogenen Daten umfassend informieren. Alle relevanten Informationen können Sie in der Datenschutzerklärung des BSI nachlesen. * (Pflichtangabe)

☐ Die Datenschutzerklärung habe ich zur Kenntnis genommen.

SEITENANFANG

Vielen Dank,

die Meldung zu Schwachstellen und Sicherheitslücken ist bei uns eingegangen.

Nutzung der Informationen

Die übermittelten Informationen zu Sicherheitsvorfällen werden vertraulich behandelt und zur Erstellung von IT (Informationstechnik)-Lagebildern genutzt. Sollten Organisationen durch den Melder mit Namen genannt werden, so wird auch der Name der Organisation durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) vertraulich behandelt. Vor der Verwendung der Informationen durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) werden alle Namen sowie personen- und organisationsbeziehbare Daten anonymisiert.

An das BSI (Bundesamt für Sicherheit in der Informationstechnik) gemeldete Sicherheitslücken von IT (Informationstechnik)-Produkten werden im "Responsible Disclosure"-Verfahren an den Hersteller des Produktes weitergeleitet. Die Weiterleitung erfolgt anonymisiert.

Sollte durch eine über den Cyber-Raum ausnutzbare Sicherheitslücke eine Gefahr für die Verfügbarkeit, Vertraulichkeit oder Integrität von IT (Informationstechnik)-Systemen einer Organisation bestehen, so wird diese vom BSI (Bundesamt für Sicherheit in der Informationstechnik) über die Sicherheitslücke informiert. Die Warnung erfolgt anonymisiert.

Überprüfbarkeit der Angaben

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) behält sich vor, eine über die Meldestelle abgegebene Meldung erst zu plausibilisieren. Damit soll verhindert werden, dass falsche oder fehlerhafte Meldungen die Aussage der Lagebilder beeinträchtigen. Für die Plausibilisierung kann es notwendig sein, mit dem Melder in Kontakt zu treten.

Ähnliche Themen

Onlineformular für Schwachstellen

Zurück zu Schwachstellenmeldung

SEITENANFANG