Joachim Lindenberg

Von: Vulnerability <vulnerability@bsi.bund.de>
Gesendet: Montag, 13. November 2023 07:26
An: [redacted]@lindenberg.one
Betreff: [CERT-Bund#2023110828002645] Ihre Meldung an das CERT-Bund
Anlagen: pgp_sign.asc

Sehr geehrter Herr Lindenberg,

Nach eingehender Prüfung Ihrer Meldung werden wir hierfür kein CVD-Verfahren einleiten, da sich Ihre Schwachstellenmeldung nicht an die in der CVD-Richtlinie des BSI festgeschrieben Grundsätze hält. Demnach wurden nicht ausreichend Informationen zur Validierung der gemeldeten Schwachstelle bereitgestellt.

Gerne gehen wir im Folgenden auf die einzelnen Punkte Ihrer Mitteilung ein, um Ihnen Gelegenheit zu geben, auf mögliche Missverständnisse auf Basis der unzureichend zur Verfügung gestellten Informationen einzugehen:

Ad 1: "OpenPGP Web Key Directory hat eine nicht ausdrücklich genannte Abhängigkeit zu DNSSEC über den TXT-Record (Abschnitt 3.1 des Drafts, s.a. GnuPG: Web Key Directory (WKD) einrichten) und durch den zweistufigen Mechanismus openpgpkey.example.org vs. example.org. Immerhin verwenden einige Schlüsselserver DNSSEC. Unklar ist jedoch, ob das auch bei den Clients der Fall ist."

Einschätzung CERT-Bund:
Eine Abhängigkeit zu DNSSEC kann hier nicht erkannt werden. Tatsächlich kann sowohl mit als auch ohne DNSSEC bei fremder Kontrolle der DNS-Antworten eine Denial-of-Service-Situation herbeigeführt werden, die im Threatmodel nicht relevant ist. Eine Beschreibung des vermuteten Sicherheitsproblems entsprechend der Kriterien der CVD-Richtlinie des BSI wäre hier hilfreich, mögliche Missverständnisse auszuräumen.

Ad 2: "Auf "WKD as a Service" (https://keys.openpgp.org/about/usage#wkd-as-a-service) steht, ein CNAME reiche. Dass der Server an den delegiert wird ein passendes Zertifikat haben muss, steht nicht da. Tatsächlich zeigt "gpg -v --auto-key-locate clear,wkd,nodefault --locate-key noreply@lindenberg.one" eine Meldung "gpg: (further info: bad cert for 'openpgpkey.lindenberg.one': Hostname does not match the certificate)" ohne jedoch abzubrechen. Unklar ist, ob Programme wie Thunderbird dann abbrechen oder Schlüssel akzeptieren."

Einschätzung CERT-Bund:
Da das Labor-Setup nicht ausreichend beschrieben wurde und zwischenzeitlich Änderungen vorgenommen wurden, liegt folgender Umstand nahe: die "Advanced"-Methode ist mit dem genannten Fehler abgebrochen, da hier ein Wildcard-Server mit dem falschen Zertifikat geantwortet hat; die "Direct"-Methode hat dann den Schlüssel abgerufen. Grundsätzlich basiert das Vertrauen in WKD auf dem TLS-Zertifikat der HTTPS-Verbindung, mit der der Schlüssel erhalten wird. Sollte hier tatsächlich keine oder unzureichende Validierung stattfinden, wäre eine Beschreibung des Problems entsprechend der Kriterien der CVD-Richtlinie des BSI notwendig, um das Problem genauer zu betrachten. Abseits davon verwendet z.B. Thunderbird die API von GnuPG, sodass das Verhalten identisch sein sollte.

Ad 3: "Aussagen zu Caching oder Key-Validierung fehlen bei OpenPGP Web Key Directory, das Löschen eines Schlüssels ist nicht vorgesehen, man muss ihn wohl durch einen zurückgerufenen ersetzen. DSGVO-konform ist das nicht."

Einschätzung CERT-Bund:
WKD beschreibt ein Verfahren zur Zugänglichmachung von öffentlichen Schlüsseln. Inwiefern Clients diese Schlüssel Cachen, zusätzlich zum durch WKD generierten Grundvertrauen validieren oder löschen ist nicht Gegenstand von WKD und außerhalb der Kontrolle von WKD-Betreibern. Ein konkretes Problem mit WKD ist an dieser Stelle nicht erkennbar.

Ad 4: "Das BSI schreibt in https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/EasyGPG/easy-

gpg_node.html#:~:text=Der%20Schl%C3%BCssel%20wird%20lokal,
der Schlüssel wird lokal im "Schlüsselbund" des Absenders gespeichert und kann zukünftig ohne Abfrage beim E-Mail Anbieter benutzt werden – im Widerspruch zu Standardanforderungen in CON.1.A4 des Grundschutz Kompendium (Edition 2023)."

Einschätzung CERT-Bund:
Ein hier implizierter Widerspruch kann nicht erkannt werden. Die in CON.1.A4 (2023) beschriebenen Anforderungen sind Konfigurationsoptionen des Clients und nicht Teil von WKD. Zusätzlich scheint die Default-Einstellung von GnuPG auch nicht im Widerspruch mit den Anforderungen an die Konfiguration zu stehen. Abseits davon sind nicht alle Zielgruppen des BSI an den Grundschutz gebunden. So kann es vorkommen, dass Hinweise die insb. an solche Zielgruppen gerichtet sind, nicht in vollem Umfang grundschutzkonform sind.

Ad 5: "Bei keys.openpgp.org, Mailvelope Key Server und OpenPGP Web Key Directory (Draft) findet die Validierung bzw. der Schlüsseltausch per Email statt – kann also nur so sicher sein, wie die zugrundeliegende SMTP-Kommunikation. SMTP-DANE oder DKIM wird leider nicht gefordert. Ein Angreifer, dem es gelingt, die Emailkommunikation zu übernehmen, kann eigene Schlüssel veröffentlichen und damit erreichen, dass Signaturen des angegriffenen Benutzers ungültig sind und der angegriffene Benutzer eingehende Mails nicht mehr lesen kann."

Einschätzung CERT-Bund:
In der Tat ist das im Threat Model von WKD angenommene Vertrauen in den E-Mail-Dienstleister und dessen korrekte Dienste-Konfiguration notwendig. Inwiefern DKIM hier von Vorteil sein sollte, ist nicht ausgeführt und auch nicht erkennbar. DANE kann einen zusätzlichen Vertrauensschutz für die TLS-Verbindung darstellen; das von WKD eingeräumte Vertrauen für Schlüssel ist allerdings verhältnismäßig niedrig, sodass der Aufwand (i.e. v.a. DNSSEC) nicht im Verhältnis zum Schutzzweck zu stehen scheint.

Ad 6: "Einige Anbieter erzeugen das Schlüsselpaar und kennen damit auch den privaten Schlüssel – was Missbrauch durch den Anbieter ermöglicht. Darüberhinaus kann der Betreiber des Schlüsselservers (meist der Betreiber der Emaildomäne) einen Schlüssel ändern – das würde auffallen – oder als The Additional Decryption Subkey hinzufügen und dann mitlesen – ggfs. im Rahmen staatlicher Telekommunikationsüberwachung."

Einschätzung CERT-Bund:
Fremderzeugte Schlüssel erlauben grundsätzlich Missbrauch. Dies ist kein Problem von WKD. WKD sieht vor, den zugesandten öffentlichen Teil privat erzeugter Schlüssel nach Prüfung zu veröffentlichen, und nicht selbst für Nutzende Schlüsselpaare zu erzeugen. Ansonsten sieht das Threat Model von WKD vor, dass die auffällige Konfigurationsänderung durch einen maliziösen E-Mail-Provider die für WKD grundlegende Vertrauensbasis zwischen Providee und Provider entfernt.

Ad 7: "Alle Systeme machen die öffentlichen Schlüssel automatisiert abrufbar, was die Benutzerfreundlichkeit stark verbessert, aber auch Spammern ermöglicht, verschlüsselte Spam zu senden, die dann nicht im Spamfilter erkannt werden kann."

Einschätzung CERT-Bund:
Sollten die Schlüssel im WKD automatisiert in akzeptabler Zeit enumerierbar sein, liegt hier eine Fehlkonfiguration des Providers vor; WKD sieht vor, dass nur mit Kenntnis der E-Mail-Addresse ein Schlüssel bezogen werden kann, da die abgefrage E-Mail-Adresse für die Abfrage gehasht werden muss - was eine erhebliche Verbesserung zu vor WKD verwendeten Keyserver-Methoden darstellt.

Ihre Schwachstellenmeldung qualifiziert sich nicht für die Aufnahme in die Hall-of-Fame des BSI.

Wir bitten um Ihr Verständnis und bedanken uns für Ihre Meldung und den damit verbundenen Beitrag, die IT-Sicherheit im Produkt/der Anwendung zu verbessern.

Mit freundlichen Grüßen
das Team CERT-Bund

Im Auftrag

--
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 08.11.2023 17:15 (Europe/Berlin) wrote Vulnerability:
*** 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 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 9.4 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