Maximilian Baehring
Hoelderlinstrasse 4
D-60316 Frankfurt am Main
Fon: +49 / (0)69 / 17320776
Fax: +49 / (0)69 / 67831634
E-Mail: maximilian@baehring.at

Maximilian Baehring Hoelderlinstrasse 4 D-60316 Frankfurt/M.

Rechtsanwalt
Kai Guthke
Sandweg 7

D-60316 Frankfurt a.M.

Frankfurt/M., 14. März 2016

EILT!

Sehr geehrter Herr Guthke

letzte Woche erreichten mich mal wieder gefälschte Fehlermeldungen hinischtlich der EZB Zertifikate. Anscheinend sind die Österreicher zu dämlich die Konfigration von SSL auf Wildcard-DNS zu verstehen. Ich füge diese Mails bei. Ich erpare Ihnen die Details meiner mehrseitigen Antworten. (Cipherwahl ist Clientsache, Wildcard-DNS).

UND JETZT KOMMTS:

Seit Erhalt dieser angeblichen Regierungs-Emails werden auf meinem Rechner Beweisfotos und Tondateien (Telefonmitschnitte wie sich die Polizei weigert Hilfe zu Leiten) wie von Geisterhand geschreddert.

Ich arbeite seit meinem 15. Lebensjahr mit Computern und bin Profi. Es liegt nicht an den Platten (daran daß es mehrere an unterschiedlichen Platten-Controllern sidn sieht man daß eien Fehlfunktion diesr ausgeschlossen ist) oder dem PC. (Backups funktionieren).

Meine Kontakte beim Areitskreis Vorratsdatenspeicherung, der Piratenpartei (verfassungsschutz unterwandert)/dem Chaos Compuzter Club CCC hatten schonmal etwas vermutet was Sie den „Bundestojanerr" nennen. Bedenken Sie daß ich mich im Datenschutz-Clinch mit der EZB befinde also mächtige Feinde habe (liegt Ihnen vor).

Passen Sie auf sich und ihre Daten auf.

Mit freundlichem Gru&SZlig;

Maximilian Bähring

Subject: [CERT.at #559994] Insecure protocol support (SSLv2/Port 443/TCP) in AS 34568
From: "Stephan Richter via RT" <team@cert.at>
Date: 07.03.2016 22:58
To: abuse@hosting-server.cc

(English version below)

Sehr geehrte Netzbetreiber,

an den im Anhang genannten IP-Adressen aus Ihrem AS wird anscheinend auf Port 443/TCP das obsolete Protokoll SSLv2 unterstützt. Wegen der damit verbundenen Risiken (Stichwort DROWN-Attacke), siehe z.B.

https://cert.at/services/blog/20160302151126-1688.html

wird empfohlen SSLv2 vollständig zu deaktivieren.

Bei der Gelegenheit sollte man ggf. auch gleich das Abdrehen von SSLv3 in Erwägung ziehen.

Bitte Ihren Richtlinien gemäss behandeln bzw. Ihre Kunden entsprechend zu informieren.

Sollte diese Mail inkorrekte Daten beinhalten, so freuen wir uns wenn Sie uns dies mitteilen, sodass wir unsere Berichte in Zukunft verbessern können.

Mit freundlichen Grüßen
CERT.at

(English version)

Dear network owner,

find attached the IP addresses of Webservers in your network apparently supporting the obsolete and insecure SSLv2 protocol on port 443/TCP.

It is highly recommended to completely disable SSLv2 (and, if possible, SSLv3 as well).

Please act according to your own policies.

Kind Regards
CERT.at
--
// CERT Austria - http://www.cert.at/ - T: +43 1 5056416 78
// an Initiative of nic.at GmbH - http://www.nic.at/
// Firmenbuchnummer 172568b, LG Salzburg

SSLv2HTTPS.csv

```
ip,timestamp,port,nr_at_domains,domain_examples
194.126.239.78,2016-03-06 06:00:26 CET,443,1,baehring.at
```

Attachments:

SSLv2HTTPS.csv	107 bytes

Subject: [CERT-Bund#2016030328002709] Für DROWN-Angriffe verwundbare Server in AS21158
From: CERT-Bund Reports <reports@reports.cert-bund.de>
Date: 03.03.2016 15:05
To: abuse.klinik-dr-baumstark@reiki-direkt.de

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

[CERT-Bund#2016030328002709]

Sehr geehrte Damen und Herren,

der sogenannte "DROWN"-Angriff (Decrypting RSA with Obsolete and Weakened eNcryption) ermöglicht einem Angreifer, zuvor aufgezeichnete gesicherte TLS-Verbindungen zu entschlüsseln und damit vertrauliche Kommunikations-inhalte auszuspähen. Durch Senden einer großen Zahl speziell präparierter Handshake-Nachrichten an einen SSLv2 unterstützenden Server können die verwendeten Verbindungsschlüssel in Erfahrung gebracht werden. Ebenso kann ein Angriff auch gegen mehrere, den gleichen privaten Schlüssel nutzende Server gestartet werden, solange mindestens einer davon noch SSLv2 unterstützt.

In einer allgemeinen Variante von DROWN, die mit hohem Rechenaufwand verbunden ist, wird für den Angriff eine Schwachstelle von SSLv2 genutzt. Das Risiko für einen erfolgreichen DROWN-Angriff wird jedoch durch zwei Schwachstellen von OpenSSL deutlich erhöht:

1. OpenSSL Versionen vor 1.0.2f bzw. 1.0.1r ermöglichen DROWN auch mit deaktivierten SSLv2-Kryptoalgorithmen. Der notwendige Verbindungsaufbau zu einem Server benötigt lediglich SSLv2-Unterstützung.
2. Eine Vielzahl der für DROWN-Angriffe anfälligen Server nutzen zudem immer noch OpenSSL in Versionen vor 1.0.2a, 1.0.1m, 1.0.0r bzw. 0.9.8zf. Diese Versionen weisen eine Sicherheitslücke auf, die die Ausführung des Angriffs weiter vereinfacht.

Von den Entdeckern der Schwachstelle durchgeführte Scans zeigen, dass noch immer ein großer Teil der weltweiten Server SSLv2 unterstützt und damit anfällig für einen DROWN-Angriff ist.

Zum Schutz vor DROWN-Angriffen muss sicher gestellt werden, dass privates Schlüsselmaterial nicht in Verbindung mit Serveranwendungen verwendet wird, welche SSLv2 zulassen. Neben Webservern gehören dazu zum Beispiel SMTP-, IMAP- oder POP-Server sowie jede andere Anwendung, die SSL/TLS unterstützt. Weitere Informationen zu DROWN und Empfehlungen zur Absicherung von Servern gegen DROWN-Angriffe finden Sie unter [1]. Um die im Kontext von DROWN stehenden Schwachstellen in OpenSSL zu schließen, werden Sicherheitsupdates in Form der neuen Versionen 1.0.2g und 1.0.1s zur Verfügung gestellt [2].

CERT-Bund hat von den Entdeckern der Schwachstelle eine Liste von Servern in Deutschland erhalten, welche im Rahmen der Scans für einen DROWN-Angriff verwundbar waren. Aus diesen Daten senden wir Ihnen nachfolgend eine Liste betroffener Server in Ihrem Netzbereich. Der Zeitstempel gibt an, wann der Server geprüft und eine Verwundbarkeit festgestellt wurde.

Wir möchten Sie bitten, den Sachverhalt zu prüfen und entsprechende Maßnahmen zu ergreifen bzw. Ihre Kunden zu informieren.

Referenzen:

[1] The DROWN Attack:
    <https://drownattack.com>
[2] OpenSSL Security Advisory [1st March 2016]
    <https://mta.openssl.org/pipermail/openssl-announce/2016-March/000066.html>

Diese E-Mail ist mittels PGP digital signiert. Informationen zu dem
verwendeten Schlüssel finden Sie auf unserer Webseite unter:
<https://www.cert-bund.de/reports-sig>

Bitte beachten Sie:
Dies ist eine automatisch generierte Nachricht.
An die Absenderadresse kann nicht geantwortet werden.
Bei Rückfragen wenden Sie sich bitte an <certbund@bsi.bund.de>.

Liste der betroffenen Server in Ihrem Netzbereich:

Format: ASN | IP | Port | Zeitstempel

 21158 | 193.109.132.10 | 443 | 2016-02-09T00:30:51-05:00
 21158 | 193.109.132.11 | 443 | 2016-02-09T13:58:59-05:00
 21158 | 193.109.132.12 | 443 | 2016-02-08T23:32:53-05:00

Mit freundlichen Grüßen
Team CERT-Bund

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat C21 - CERT-Bund
Godesberger Allee 185-189
D-53175 Bonn

-----BEGIN PGP SIGNATURE-----
Comment: Key verification: <https://www.cert-bund.de/reports-sig>

iQIcBAEBCAAGBQJW2ETDAAoJEMSjo7JqGA8c99gQAIak3xDfwOhaNpTz2aljyYP1
gKAq2e9FMe4/MHMf9fx0k5eyHP9LaSG1XX7MIN+TA2D3Montfu8Bnt6WlkPlQmdD
1I6t2aw0I5E41xa9CrHvJ/xUFrdnFk6+D/0JN2xfsGY8gTVRvm7Tpf2D2uqrMzRr
rPaIjB0tBN8eZboxbMr4igFiJz8vFlNHDljEISkLN0qGEhvhljJuekZ9FYUOespW
B6SP/7o3jyyfgP0eL6/Z4Zg4wiXc2LFLGvtirmGuuRER/sopk4m4EA9WJhpyFyB/
QXMwKZp6kfZrdRADjfdsxviQJPpYIKdPA7gFjGCCajCHIIc3Z3Loi+DMR2KA2VlX
nKJsb2fYiQMwpCH4XcWlHAyQikzFbit9AGOCfS9uzi8dsx6+1CN7AEpujio+bYGK
9fcQIZv840eM0ULmbCU/EOA71Vbm6gVSvm5aFhZWbkd7CqbqPLR0McXwyJ6X3dig
OBrfeuldJ/bJT35PSg0kMqdLNOoGsjnMkwaBpEWJPOiXbS4w6seRLDyTwXQFMOcb
fsw6JJykeyogjTR4+gux2uWEfUbxKmp89/eOe/Y1EG57sL7HXIAoSJKLKfR4H6jg
wxuHubC8EvIxC7jVByGm8K1nD46rbubh7PD3b21TuMBETx24nLGIYXCdZRUkaQGu
/jtWI93UtAraZyVnhgib
=K5Hy
-----END PGP SIGNATURE-----