Fwd: AW: Weitere technische Informationen zu Hacker-Angriff

Von: [redacted] <vorzimmerpvp@bsi.bund.de> (Leitungsstab)
An: GPLeitungsstab <leitungsstab@bsi.bund.de>
Datum: 19.10.2018 10:27

LKn,

Euch zur Kenntnis.

Viele Grüße
Im Auftrag
[redacted]

_____ weitergeleitete Nachricht _____

Von: gerhard.schabhueser@bsi.bund.de
Datum: Samstag, 29. September 2018, 21:33:12
An: [redacted]@fb.com
Kopie:
Betr.: AW: Weitere technische Informationen zu Hacker-Angriff

> Lieber [redacted]
> vielen Dank für das Update
> Beste Grüße
> Gerhard schabhüser
>
> Gesendet von meinem BlackBerry 10-Smartphone.
> Originalnachricht
> Von: [redacted]
> Gesendet: Samstag, 29. September 2018 19:01
> An: gerhard.schabhueser@bsi.bund.de
> Betreff: Weitere technische Informationen zu Hacker-Angriff
>
> Lieber Herr Schabhüser,
>
>
> unten stehend sende ich Ihnen eine kurze technische Zusammenfassung, wie
> der Angriff verlaufen ist. Wir werden auch zeitnah eine deutschsprachige
> Version der Angriffsbeschreibung zur Verfügung stellen.
>
> Earlier this week, we discovered that an external actor attacked our
> systems and exploited a vulnerability that exposed Facebook access tokens
> for people’s accounts in HTML when we rendered a particular component of
> the “View As” feature. The vulnerability was the result of the interaction
> of three distinct bugs:
>
> First: View As is a privacy feature that lets people see what their own
> profile looks like to someone else. View As should be a view-only
> interface. However, for one type of composer (the box that lets you post
> content to Facebook) — specifically the version that enables people to wish
> their friends happy birthday — View As incorrectly provided the opportunity
> to post a video.
>
> Second: A new version of our video uploader (the interface that would be
> presented as a result of the first bug), introduced in July 2017,
> incorrectly generated an access token that had the permissions of the
> Facebook mobile app.
>
> Third: When the video uploader appeared as part of View As, it generated
> the access token not for you as the viewer, but for the user that you were
> looking up.
>
> It was the combination of these three bugs that became a vulnerability:
> when using the View As feature to view your profile as a friend, the code

> did not remove the composer that lets people wish you happy birthday; the
> video uploader would generate an access token when it shouldn't have; and
> when the access token was generated, it was not for you but the person
> being looked up. That access token was then available in the HTML of the
> page, which the attackers were able to extract and exploit to log in as
> another user.
>
> The attackers were then able to pivot from that access token to other
> accounts, performing the same actions and obtaining further access tokens.
>
> To protect people's accounts, we've fixed the vulnerability. We have also
> reset the access tokens of the almost 50 million accounts we know were
> affected and we've also taken the precautionary step of resetting access
> tokens for another 40 million accounts that have been subject to a View As
> look-up in the last year. Finally, we've temporarily turned off the View As
> feature while we conduct a thorough security review.
>
> Beste Grüße,
>
> [redacted]
>
>
> Facebook | Instagram
>
> [redacted] | Manager Public Policy
> Mobile +49 [redacted]
> E-Mail [redacted]@fb.com
> Facebook Germany GmbH
> "Sony Center" | Kemperplatz 1A | 10785 Berlin
>
> Erfahren Sie mehr über Facebook in Deutschland unter:
> https://deutschland.fb.com/
>
> HRB 111963 Amtsgericht Hamburg
> Geschäftsführer Susan Taylor, Shane Crehan, David William Kling

--
[redacted]

Vorzimmer P/VP
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 -189
53175 Bonn
Telefon: +49 228 99 9582-[redacted]
Fax: +49 228 99 10 9582-5420
E-Mail: vorzimmerpvp@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de