Zoomご利用のお客様　各位

SE20-22SE-004
2020年4月6日
エイチ・シー・ネットワークス株式会社

Zoom　Windows及びiOSクライアントにおける脆弱性問題の対応について

平素は格別のご高配を賜り、厚く御礼申し上げます。
また日頃よりZoomクラウドサービスをご利用頂き、誠にありがとうございます。

Zoomミーティングクライアントの脆弱性に関する記事が、インターネット上に公開されていますが、Zoom Video Communications, Inc及びその日本法人であるZVC Japanは、以下2件の事象について、アプリケーションのバージョンアップによる対策を行いましたので、以下のご対応を実施いただけますようお願いいたします。

1)事象1
【事象】
iOSクライアントで使用しているFacebook SDKがユーザの意図しないデータ送信を行う事象。(iOS版クライアント)
【対策】
ZoomミーティングiOS（iPhone及び一部のiPad）版をご利用中のお客様における最新版のアプリケーション（Ver.4.6.9）へのアップデート
※日本標準時(JST) 2020年3月28日（土) 7:30　時点で、問題が解消された最新バージョンのアプリケーションが提供されております。

2)事象2
【事象】
グループチャットのリンク共有機能を悪用した場合、リンクをクリックした人のWindowsのネットワーク認証情報が漏えいする可能性がある。(Windows版クライアント)
【対策】
ZoomミーティングWindows版をご利用中のお客様における、最新版のアプリケーション（Ver.4.6.9）へのアップデート。
※日本標準時（JST）2020年4月3日（金) 7:30　時点で、最新バージョンのアプリケーションが提供されております。
その他のOS(MAC OS)につきましても、Ver.4.6.9へのバージョンアップをお願いします。

Zoom Video Communications, IncのEric S. Yuan CEOは現地時間2020年04月01日、同社のZoomサービスに複数の脆弱性やオープンなオンライン会議やクラスをハイジャックし、嫌がらせを行う「Zoom-Bombing」が発生していることに対して謝罪し、今後90日間は、社内のリソースを集約し、セキュリティ問題の修正に専念することと、そのプロセスについて透明性を図り進めると発表しています。なお、最新のセキュリティポリシーについは、以下のURLをご覧ください。
https://zoom.us/jp-jp/privacy.html

弊社と致しましては、お客様に以下の点についてご注意頂き今後Zoomをご利用頂くことを、強く推奨いたします。

① Zoomクラウドサービスから最新パッチ提供のアナウンスがPCや各種デバイス上に表示された場合は、速やかにパッチの適用を行い最新Versionでご利用ください。
② 毎回開催される会議IDと会議パスワードは、固定する運用ではなく毎回ランダム生成してご利用ください。
・会議IDは、マイパーソナルミーティングID（PMI）を利用せず、自動的に生成を選択する
・会議パスワードの設定は必須選択とし、最長10桁のパスワードを設定する。
③ 2時間以上の長時間接続を想定している会議は、会議時間を短く区切り再接続しなおしてご利用ください。

弊社は今後もZoom Video Communications, Inc及びZVC Japan、販売代理店と連携し、より安全でより良いサービスをご提供できますよう努力してまいります。

以上