ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●パスワード管理サービス「LastPass」、不正アクセスで暗号化状態のパスワード等が流出

https://gigazine.net/news/20221223-lastpass-password-hacking/
https://gigazine.net/news/20221201-lastpass-hackers-accessed-customer-data/
https://news.mynavi.jp/techplus/article/20221223-2544442/
https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

このニュースをザックリ言うと･･･

- 12月22日(現地時間)、パスワード管理サービスLastPassより、8月および12月1日に発生した不正アクセスにより、暗号化されたパスワードを含むユーザーのデータが奪取されていたと発表されました。

- 同社では8月に不正アクセスを受けた時点でその旨を発表しており、その際にはソースコードや技術情報の一部が流出し、ユーザーに関連する情報の流出はなかったとしていました。

- しかしこの時点で流出した情報をもとに12月に再び不正アクセスが発生し、ユーザーの個人情報と、ユーザーが保存したパスワードが暗号化したデータが奪取されたことが今回発表されています。

- なお暗号化されたパスワードデータは、ユーザーが入力するマスターパスワードを基にした鍵で保護されているとのことです。

AUS便りからの所感等

- LastPassはオンライン上でパスワードを管理するサービスとしてもっとも著名なものの一つであり、これまでも度々攻撃者からターゲットとされていました。

- 攻撃者は8月の不正アクセスで得た情報をもとにLastPass従業員のアカウントを奪取し、バックアップデータが保存されたクラウドストレージにアクセスしたとみられ、本番環境は影響を受けていないとのことです。

- マスターパスワードが、他のWebサービス等と共有していない、十分に強力なパスワードである限りは、暗号化が解除される可能性は低いですが、LastPassではマスターパスワードを聞き出すフィッシングの可能性に注意を呼び掛けています。

- LastPassと同様のサービスとしてBitWardenや1passwordが知られており、またサービスが所有するサーバーにデータを保存することが心もとないのであれば、ローカル上にのみ、あるいは自分が契約したクラウドストレージ上にパスワードを保存できるツールとしてKeePass等がありますが、暗号化したデータが万が一奪取された場合を考え、マスターパスワードだけは決して簡単な文字列を使わないよう留意が必要です。

GIGAZINE

2022年12月23日 11時03分　セキュリティ

パスワード管理アプリ「LastPass」のパスワードや個人情報が盗まれていたことが判明

パスワード管理アプリ「LastPass」では、2022年8月の不正アクセスによってソースコードが盗まれて以降、ハッカーによる顧客データへの不正アクセスが発生しています。LastPassは2022年12月22日に不正アクセスによってユーザーの個人情報やパスワードなどのデータが漏えいしたことを発表しています。

Notice of Recent Security Incident - The LastPass Blog
https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

LastPass says hackers stole customers' password vaults | TechCrunch
https://techcrunch.com/2022/12/22/lastpass-customer-password-vaults-stolen/

LastPass users: Your info and password vault data are now in hackers' hands | Ars Technica
https://arstechnica.com/information-technology/2022/12/lastpass-says-hackers-have-obtained-vault-data-and-a-wealth-of-customer-info/

●大学学生・教職員ら5,288人分の個人情報流出か…名誉教授のメールアカウント乗っ取られる

https://www3.nhk.or.jp/lnews/kumamoto/20221213/5000017737.html
https://mainichi.jp/articles/20221213/k00/00m/040/261000c
https://www.pu-kumamoto.ac.jp/news/post-23585/

このニュースをザックリ言うと･･･

- 12月13日(日本時間)、熊本県立大学より、同大学が不正アクセスを受け、個人情報が流出した可能性があると発表されました。
- 被害を受けた可能性があるのは、同大学の学生・教職員らのべ5,288人分の個人情報(名前・メールアドレスおよび電話番号等)とされています。
- 同大学の名誉教授のメールアカウントが8月30日以降海外から不正にログインされ、12月6日～7日に当該アカウントから不審なメールの送信が確認されたことから発覚したとしています。

AUS便りからの所感

- 不審なメールは46件が相手に送信、一方で1,230件が遮断されてエラーメールが返っており、このエラーメールについて名誉教授から「出した覚えのないメールが多数返ってくる」と連絡があったのが発覚のきっかけとみられます。
- 大学におけるメールアカウントへの不正アクセス事案は、11月にも創価大学でスパムメール送信に悪用された事例があります(AUS便り 2022/11/29号参照)。
- 今回の事例ではメールアカウントに多要素認証が設定されていた一方、名誉教授のアカウントは特例で多要素認証が設定されず、パスワードも簡単なものとされていたことが、不正ログインが成立した原因とされています。
- 外部への不審な内容のメール送信を遮断するよう、メールサーバー自体もしくはその前面にUTMの設置等ソリューションを導入すること、また多要素認証の導入が容易ではない場合は、少なくとも不審なログイン試行を検知・遮断する設定を行うことを推奨致します。

NHK

県立大 不正なアクセスで５０００人超の個人情報漏えいか

12月13日　18時23分

熊本県立大学は、名誉教授のメールアカウントに外部から不正なアクセスがあり、学生の氏名やメールアドレスなどのべ５０００人を超える個人情報が漏えいした疑いがあると発表しました。

熊本県立大学が１３日開いた会見によりますと、今月７日、名誉教授から「出した覚えのないメールが多数返ってくる」などと大学に相談がありました。

大学が調査したところ、今月６日から翌日にかけて名誉教授のメールアカウントから不審な英文メールが４６件勝手に送信されていたほか、ことし８月３０日以降、教授のアカウントに、およそ１０００件にのぼる海外からの不正なアクセスが検出されたということです。

● Linuxカーネル5.15以降に重大な脆弱性、バージョン確認と対策を

https://japan.zdnet.com/article/35197887/
https://www.zerodayinitiative.com/advisories/ZDI-22-1690/

このニュースをザックリ言うと･･･

- 12月22日(現地時間)、トレンドマイクロ社が運営する脆弱性発見コミュニティ「Zero Day Initiative」より、Linuxカーネルに危険度の高い脆弱性(ZDI-CAN-17816)が存在すると発表されました。
- 脆弱性はカーネルバージョン5.15に組み込まれたSMB(主にWindowsでファイル共有に使用されるプロトコル)サーバー機能「ksmbd」に存在し、ksmbdが有効になっているサーバー上でリモートから任意のコード実行が可能になるとされています。
- 8月に脆弱性を修正した5.15.61がリリースされており、5.15系を使用している場合には速やかに適用が推奨されます(なお5.14系以前および6.0系以降には脆弱性はありません)。

AUS便りからの所感

- カーネル5.15系を採用しているLinuxディストリビューションは「Ubuntu 22.04以降」「Deepin 20.3」「Slackware 15」が挙げられています。
- 「Debian」や「Red Hat Enterprise Linux(およびCentOS・Rocky・Alma等派生)」では5.14系以前を採用しているため、ディストリビューション提供のカーネルを使用している限り影響は受けませんが、独自に5.15系カーネルをコンパイルして導入している場合は同系列あるいは6.0系以降の最新バージョンをインストールしてください。
- 内部ネットワークに対してSMBサービスを提供している場面で、内部に攻撃者が侵入した場合に脆弱性を悪用した攻撃を受けることを想定し(Linuxのみならず Windowsサーバーや NASでも同様です)、根本的な対策として各種ソフトウェアを最新バージョンに保ち、あるいはセキュリティパッチの適用を確実に行うこと、可能であればUTMを前面に設置する等して不審なアクセスを遮断できるネットワーク構成とすることが肝要です。

ZDNet Japan

Linuxカーネルの「ksmbd」に深刻なセキュリティ脆弱性

Steven J. Vaughan-Nichols (Special to ZDNet.com) 翻訳校正: 編集部　2022-12-26 10:42

Linuxのシステム管理者であれば誰しもが、ホリデーシーズン目前に、Linuxカーネルに深刻なセキュリティ脆弱性が発見されたというニュースは目にしたくはないはずだ。とは言うものの、トレンドマイクロが運営する脆弱性発見コミュニティーであるZero Day Initiative（ZDI）は米国時間12月22日、Linuxカーネルに潜むセキュリティ脆弱性を発見したと報告した。この脆弱性を悪用することで、認証されていないリモートユーザーであっても機密情報を窃取したり、脆弱性を抱えたシステム上でコードを実行できるようになる。