サイバーセキュリティ通信 Vol.8

令和４年９月

WordPressの脆弱性について

WordPressとは？

ウェブサイトの構築に使用されるオープンソースソフトウェアです。
全世界のウェブサイトの約4割で利用されており、日本国内においても高いシェアを占めています。

今回発見されたぜい弱性（CVE-2022-3180）

ウェブサイト管理者がサイトのバックアップやサイトで利用する拡張機能（プラグイン）の管理等を行うために利用する **WPGateway** と呼ばれる拡張機能に脆弱性が発見されました。
このぜい弱性を悪用されると、攻撃者によって管理者権限を持つ不正なユーザを追加され、**ウェブサイトを乗っ取られる危険** があります。

ウェブサイトが侵害されている場合、
rangex
という管理者権限が作成されています。

自社のウェブサイトはWordPressで構築されていませんか？

実際に多くのウェブサイトに攻撃が行われていることから、下記の対策をお願いします。

- **rangex** という管理者権限が作成されていないか、確認してください。
- **WPGateway** を削除してください。
  ※修正プログラムが配布されるまで、一旦、削除してください。
- 拡張機能も含めてWordPressの最新化を行ってください。

＜参考＞　PSA:Zero-Day Vulnerability in WPGateway Actively Exploited in the Wild
https://www.wordfence.com/blog/2022/09/psa-zero-day-vulnerability-in-wpgateway-actively-exploited-in-the-wild/

もし被害に遭われた際は……
警察にご相談ください。

長崎県警察本部生活安全部サイバー犯罪対策課
095-820-0110（3451・3452）

サイバー犯罪対策課
公式LINEアカウントで
情報配信中！