IIJからのお知らせ

2025年 4月 21日 (月)

お客様各位

株式会社インターネットイニシアティブ

不正アクセスに伴う情報漏えいに関するお詫びとご報告(4/21) | IIJセキュアMXサービス

拝啓　時下ますますご清祥のこととお慶び申し上げます。
平素は弊社サービスをご利用いただき、誠にありがとうございます。

IIJセキュアMXサービス（以下、SMX）におけるお客様情報の外部漏えいにつきまして、下記の通りご報告申し上げます。
お客様ならびに関係者の皆様には、多大なるご心配とご迷惑をおかけしておりますことを、深くお詫び申し上げます。

なお、ご不明な点などございましたら、お客様窓口までお問い合わせくださいますよう、お願い申し上げます。

敬具

＜ 記 ＞

不正アクセスの発生日	2024年08月03日（土）以降
不正アクセスの発覚日	2025年04月10日（木）
不正アクセスの発見の経緯と現状	2025年04月10日にSMXの一部のサービス設備において、通常の設備運用では出力されないアラートを検知いたしました。調査を進める中で、外部からの不正アクセスの形跡および不正なプログラムの実行が確認されました。 当該システムを遮断後に調査を実施した結果、お客様の情報が漏えいした可能性があることが判明しました。これを受けて設備のログ情報や侵入者が残した各種の形跡について、詳細調査を進めてまいりました。 このたび調査が完了し、その結果として漏えいした情報が特定されました。漏えいした事実が確認された情報については後述「漏えいした情報」の通りとなります。 なお、「漏えいした情報」に記載のない情報については、漏えいした事実は確認されませんでした。
漏えいした情報	• ドメイン名 • お客様送信/受信メールサーバ(IPアドレスやホスト名)
不正アクセスの原因	外部からの不正アクセスの原因は、当該システムで利用していたソフトウェアの脆弱性を悪用されたことによるものでした。この脆弱性は不正アクセス発生から発覚のタイミングでは未発見のものであり、今回の事案を通じて初めて明らかになったものです。その後、製造元による改修が完了し、04月18日にJVN(※)において緊急度の高い脆弱性として情報が公開されております。 対象となった脆弱性：JVN#22348866:"Active! mailにおけるスタックベースのバッファオーバーフローの脆弱性 緊急"(https://jvn.jp/jp/JVN22348866/index.html) ※JVN(Japan Vulnerability Notes)。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報

	ポータルサイト。脆弱性関連情報の受付と安全な流通を目的とした「情報セキュリティ早期警戒パートナーシップ」に基づいて、2004年07月よりJPCERT コーディネーションセンターと独立行政法人情報処理推進機構(IPA)が共同で運営しています。
今後の対応	再発防止に向けて、セキュリティ対策および監視体制の一層の強化を進め、サービス品質の向上とお客様からの信頼回復に全力で取り組んでまいります。
お客様へのお願い	事前にもご案内させて頂いておりますが、漏えいした情報に各種パスワード、トークンが含まれる場合は、パスワード、トークンの変更を実施いただきますようお願い申し上げます。お手数をおかけすることとなり大変申し訳ございません。

以上

※ 時刻は24時制にて記載しております。

➜ IIJからのお知らせへ ➜ お知らせトップへ

UP