

[View the original article](#)

دانش و فناوری

نقص امنیتی در اینترنت، خدمات بانکی و دولتی ژاپن را هم پس از اروپا با اختلال مواجه کرد

راديو فردا

۱۴۰۵/آبان/۰۱



اختلال‌های گسترده اینترنتی ناشی از کشف دو نقص امنیتی خطرناک در یکی از زبان‌های برنامه‌نویسی پرکاربرد جهان، پس از چند کشور اروپایی به ژاپن نیز رسید و باعث توقف بخشی از خدمات بانک‌ها، شرکت‌های هواپیمایی، راه‌آهن و نهادهای دولتی این کشور شد.

خبرگزاری رویترز روز جمعه اول آبان گزارش داد که شرکت مخابراتی سافت‌بانک ژاپن، یکی از بزرگ‌ترین اپراتورهای تلفن همراه این کشور، سامانه ارسال هشدارهای اضطراری به مشترکان خود را برای برطرف کردن این آسیب‌پذیری‌ها موقتاً غیرفعال کرده است.

این اختلال‌ها به دنبال شناسایی دو آسیب‌پذیری بسیار خطرناک در زبان برنامه‌نویسی «پی‌اچ‌پی» (PHP) رخ داده است که در بخش بزرگی از وب‌سایت‌های جهان به کار می‌رود و بسیاری از خدمات اینترنتی برای پردازش اطلاعات و پاسخ‌گویی به کاربران به آن وابسته‌اند.

افشای این نقص‌ها میلیون‌ها تلاش برای نفوذ به سامانه‌های اینترنتی را در پی داشته و شرکت‌ها و سازمان‌های بسیاری را در کشورهای مختلف وادار کرده است برای جلوگیری از حملات احتمالی، خدمات آنلاین خود را موقتاً متوقف کنند یا اصلاحیه‌های امنیتی را با فوریت نصب کنند.

در ژاپن، شرکت‌های بزرگی از جمله گروه مالی میتسوبیشی یواف‌جی، شرکت خدمات مالی نومورا، شرکت هواپیمایی آل نیپون ایرویز و شرکت راه‌آهن شرق ژاپن، بخشی از خدمات اینترنتی خود را به‌عنوان اقدام احتیاطی متوقف کرده‌اند.

وزارت دارایی، سازمان ملی مالیات و سازمان هواشناسی ژاپن نیز برخی از خدمات آنلاین خود را به‌طور موقت از دسترس خارج کرده‌اند.

گسترده‌گی این اختلال‌ها دولت ژاپن را به اتخاذ تدابیر تازه‌ای برای مقابله با تهدیدهای سایبری واداشته است.

دولت این کشور روز جمعه اعلام کرد تیمی ویژه تشکیل می‌دهد که با استفاده از هوش مصنوعی، حملات سایبری را شبیه‌سازی کند تا نقاط ضعف سامانه‌های رایانه‌ای پیش از سوءاستفاده مهاجمان شناسایی شوند.

ریوسی آکازاوا، وزیر صنعت ژاپن، با اشاره به اینکه برای موفقیت یک حمله سایبری کافی است مهاجمان تنها یک راه نفوذ پیدا کنند، گفت نهادهای مسئول امنیت اینترنت باید از دیدگاه مهاجمان به سامانه‌های خود نگاه کنند.

او تأکید کرد که مدافعان امنیت سایبری نیز باید از هوش مصنوعی استفاده کنند و با اقدامات پیشگیرانه یک گام جلوتر از مهاجمان باشند.

دامنه اختلال‌های ناشی از این آسیب‌پذیری‌ها پیشتر به چندین کشور اروپایی نیز رسیده بود.

روز چهارشنبه ۲۹ مهر، وب‌سایت‌های دولتی و خدمات اینترنتی در کشورهایی از جمله جمهوری چک، فرانسه، هلند و بلژیک، برای جلوگیری از سوءاستفاده احتمالی مهاجمان سایبری به‌طور موقت از دسترس خارج شدند.

دولت جمهوری چک اعلام کرد وب‌سایت رسمی خود را از ساعت هفت عصر چهارشنبه به وقت محلی، پس از دریافت هشدار نهاد امنیت سایبری این کشور، برای نصب به‌روزرسانی‌های ضروری تعطیل کرده است.

در فرانسه نیز شماری از وب‌سایت‌های دولتی، از جمله وب‌سایت پلیس پاریس، از دسترس خارج شدند.

در هلند نیز خدمات هویت دیجیتال و وب‌سایت پارلمان به‌عنوان اقدام احتیاطی موقتاً تعطیل شدند.

این اقدامات پس از آن انجام شد که کارشناسان امنیت سایبری هشدار دادند آسیب‌پذیری‌های تازه ممکن است به مهاجمان اجازه دهند بدون نیاز به رمز عبور یا دسترسی قبلی، به سرورهای اینترنتی نفوذ کنند.

آژانس امنیت سایبری اتحادیه اروپا نیز از سازمان‌ها و شرکت‌ها خواست هرچه سریع‌تر اصلاحیه‌های امنیتی را نصب کنند و در صورت ناتوانی در به‌روزرسانی فوری، سامانه‌های آسیب‌پذیر را موقتاً از شبکه اینترنت جدا کنند.

بیشتر در این باره:
کشف آسیب‌پذیری امنیتی با هوش مصنوعی؛
وبسایت‌های دولتی در چند کشور از دسترس خارج
شدند



نقص امنیتی PHP چیست و چرا اهمیت دارد؟

پی‌اچ‌پی یکی از زبان‌های برنامه‌نویسی قدیمی و پرکاربرد در اینترنت است که بخش مهمی از فعالیت وبسایت‌ها را در پشت صحنه مدیریت می‌کند.

برای مثال، هنگامی که کاربری وارد یک وبسایت می‌شود، اطلاعاتی را جست‌وجو می‌کند یا فرم اینترنتی را تکمیل می‌کند، ممکن است پردازش این درخواست‌ها در سرور با استفاده از پی‌اچ‌پی انجام شود.

بر اساس آمار شرکت‌های بررسی‌کننده فناوری وب، نزدیک به ۷۰ درصد وبسایت‌هایی که زبان برنامه‌نویسی مورد استفاده آن‌ها قابل شناسایی است، از پی‌اچ‌پی استفاده می‌کنند.

دو آسیب‌پذیری تازه شناسایی‌شده در این زبان برنامه‌نویسی، از نوعی هستند که ممکن است به مهاجمان امکان دهند از راه دور و بدون احراز هویت، کدهای مخرب را روی سرورهای آسیب‌پذیر اجرا کنند.

چنین دسترسی‌ای می‌تواند زمینه‌ساز سرقت اطلاعات، اختلال در خدمات یا نفوذ به بخش‌های دیگر شبکه‌های رایانه‌ای شود.

به گفته کارشناسان امنیت سایبری، این نقص‌ها از آن جهت خطرناک‌اند که مشکل در خود زبان برنامه‌نویسی وجود دارد و لزوماً به اشتباه مدیران یک وبسایت یا ضعف طراحی آن مربوط نمی‌شود.

با این حال، از دسترس خارج شدن یک وبسایت لزوماً به معنای نفوذ موفق مهاجمان به آن نیست؛ بسیاری از سازمان‌ها خدمات خود را صرفاً برای جلوگیری از سوءاستفاده احتمالی و انجام اقدامات امنیتی متوقف کرده‌اند.

توسعه‌دهندگان PHP روز چهارشنبه نسخه‌های اصلاح‌شده این نرم‌افزار را منتشر کردند و از مدیران وبسایت‌ها و شرکت‌های ارائه‌دهنده خدمات اینترنتی خواستند فوراً سامانه‌های خود را به‌روزرسانی کنند.

یکی از جنبه‌های قابل توجه این رویداد، نقش هوش مصنوعی در شناسایی آسیب‌پذیری‌هایی است که به گفته توسعه‌دهندگان، سال‌ها در نرم‌افزار پی‌اچ‌پی وجود داشته‌اند.

این نقص‌ها با کمک ابزارهای هوش مصنوعی، از جمله مدل‌های توسعه‌یافته توسط شرکت‌های اوپن‌ای‌آی و گوگل، شناسایی شدند.

اما کارشناسان امنیت سایبری هشدار می‌دهند همان فناوری که به پژوهشگران در کشف نقاط ضعف نرم‌افزارها کمک می‌کند، می‌تواند در اختیار مهاجمان نیز قرار گیرد و شناسایی راه‌های نفوذ را برای آن‌ها آسان‌تر کند.

به گفته کارشناسان، استفاده هم‌زمان مدافعان و مهاجمان از هوش مصنوعی، سرعت شناسایی آسیب‌پذیری‌ها و تلاش برای سوءاستفاده از آن‌ها را افزایش داده و اهمیت به‌روزرسانی سریع سامانه‌های اینترنتی را بیش از پیش آشکار کرده است.

