آسیب پذیری خطرناک ویندوز سرور پس از ۱۷ سال پچ شد - دیجیاتو

پیمان حسنی | چهارشنبه، ۲۵ تیر ۱۳۹۹

محققان امنیتی به شرکت‌ها هشدار داده‌اند تا ویندوز سرور را به روز کرده و از شبکه‌های خود در برابر آسیب پذیری خطرناکی که ۱۷ سال است در کدهای این سیستم عامل پنهان شده محافظت کنند.

آسیب پذیری مورد بحث که با کد CVE-2020-1350 شناسایی می‌شود، در سیستم امتیازدهی آسیب پذیری عام (CVSS)، امتیاز 10.0 یا بسیار خطرناک را دریافت کرده و در آپدیت امنیتی جدید مایکروسافت که دیروز منتشر شد رفع شده است.

این آسیب پذیری توسط محققان امنیتی شرکت Check Point کشف شده و به Microsoft Windows DNS و نرم افزار سرور مربوط می‌شود. به گفته محققان این آسیب پذیری که SigRed نام گرفته، اهمیت بالایی دارد چرا که قابلیت تبدیل شدن به کرم را داشته و می‌تواند بدون دخالت کاربر از یک سیستم آسیب پذیر به سیستم آسیب پذیر دیگر رفته و شبکه را به طور کامل آلوده کند.

هکرها با سواستفاده از این حفره می‌توانند کوئری‌های مخرب DNS را در سرورهای ویندوز DNS

ایجاد کرده و به طور کامل به زیرساخت شبکه نفوذ کنند. این آسیب پذیری در تمام نسخه‌های ویندوز سرور از سال ۲۰۰۳ تا ۲۰۱۹ وجود دارد. هکرها به واسطه این حفره کنترل سرور را به دست گرفته و توانایی دستکاری ایمیل‌ها و ترافیک شبکه، از دسترس خارج کردن سرویس‌ها، سرقت نام کاربری و رمز عبور کاربران و غیره را پیدا می‌کنند.

شرکت Check Point یافته‌های خود از این آسیب پذیری را در تاریخ ۱۹ مه (۳۰ اردیبهشت) در اختیار میکروسافت قرار دارد. این شرکت پس از تأیید این حفره و شناسایی آن به عنوان آسیب پذیری کرم شدنی، دیروز (۲۴ تیر) پچ آن را منتشر کرد.

در حال حاضر مشخص نیست وسعت سواستفاده از این آسیب پذیری تا چه حد است، اما به مدت ۱۷ سال در کدهای مایکروسافت پنهان شده بوده و به گفته شرکت امنیتی Check Point احتمال دارد در این بازه از آن سواستفاده شده باشد.

دیجیاتو