禪

یک آسیبپذیری روز صفر

شکاف امنیتی ۹۰ هزار دلاری که تمام سیستمهای ویندوز را دور میزند !

آسیبپذیریهای روز صفر بسیار مطبوع برای کاشف آن و عذابآور برای صاحب محصول نرمافزاری به شمار
میروند . اما به تازگی خبری در دنیای فناوری منتشر شده که نشان میدهد هکری موفق به کشف یک حفره
امنیتی بزرگ در تمامی پلتفرمهای ویندوز شده است . جالب آنکه این آسیبپذیری در سیستمعامل ویندوز 10
نیز قرار دارد و اکنون این هکر در نظر دارد این اکسپلویت کشف شده را به بالاترین قیمت در دنیای
زیرزمینی وب به فروش برساند .

آسیبپذیریهای روز صفر، رخنههای نرمافزاری هستند که به حمله کنندگان اجازه میدهند کنترل یک سامانه را به دست گیرند . این حملات از آن جهت روز صفر نامیده میشوند که سازنده نرمافزار از وجود آنها هیچگونه اطلاعی ندارد . این اکسپلویتها بهطرز عجیبی با قیمتهای باور نکردنی و بسیار بالا توسط مجرمان اینترنتی یا سازمانهای خاص خریداری میشود . افرادی که تمایل دارند در سکوت کامل به کنترل دستگاههای مختلف بپردازند . به همین دلیل است که دستیابی به این چنین اکسپلویتهایی همواره با استقبال بالایی در بازار سیاه روبرو میشود .

مطلب پیشنهادی

یشنهاد دانلود چند نرمافزارهای امنیتی سودمند

محافظتِ از خودِ در مقابل پلیدیهای آنلاین

اما در این مورد پیشنهاد فروش 90 هزار دلار یک اتفاق نادر است . در آسیبپذیری روز صفر جاری به نظر میرسد، مایکروسافت هیچگونه اطلاعی در مورد آن نداشته یا حداقل هیچگونه وصلهای برای آن عرضه نکرده است. فروشندهای که نام مستعار BuggiCorp را برای خود انتخاب کرده ادعا کرده است این اکسپلویت در تمامی سیستمعاملهای مایکروسافت از ویندوز 2000 گرفته تا ویندوز 10 آماده بهرهبرداری است. بر همین اساس و به دلیل با ارزش بودن این اکسپلویت تصمیم گرفته است قیمت 90 هزار دلار (تقریبا معادل 306 میلیون تومان) را برای این کشف خود پیشنهاد کند . تصویر زیر ارزشگذاری انجام شده در ارتباط با اکسپلویتهای شناسایی شده در پلتفرمهای مختلف را نشان میدهد .

ZERODIUM Payout Ranges *
LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape
Up to $500,000
Up to $100,000
Up to $80,000
Up to $50,000
Up to $40,000
Up to $30,000
Up to $10,000
Apple iOS
Android
Windows Phone
Adobe PDF Reader
Flash Player with SBX
Chrome with SBX
VM Escape
IE / Edge with SBX
Safari with SBX
Flash Player w/o SBX
ASLR Bypass
Antivirus
OpenSSL
PHP
Sendmail
Postfix
Exchange Server
Dovecot
Chrome w/o SBX
IE / Edge w/o SBX
Tor Browser
Firefox
Safari w/o SBX
Office Word/Excel
Windows Reader App
Windows
Mac OS X
Linux
IP.Suite
IP.Board
phpBB
vBulletin
MyBB
WordPress
Joomla
Drupal
Roundcube
Horde
* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.
© zerodium.com

ویدویی که توسط این هکر ضبط شده نشان میدهد حتی جدیدترین بیلد ارائه شده از ویندوز 10 نیز همچنان به این آسیبپذیری آلوده است . اما موضوعی که بیش از پیش همگان را نگران کرده است این است که این آسیبپذیری توانایی گذر از EMET که بهطور خاص توسط مایکروسافت طراحی شده است را دارد. EMET (سرنام Enhanced Mitigation Experience Toolkit) مکانیزم امنیتی یکپارچه طراحی شده از سوی مایکروسافت است که پردازههای سیستم را مورد ارزیابی قرار میدهد . این مکانیزم به گونهای طراحی شده است که در زمان رویارویی با یک پردازه با فعالیتهای غیر عادی اجرای آنرا به حالت تعلیق در میآورد . در این حالت تمامی منابع اختصاص یافته به یک پردازه بازپس گرفته میشوند . به عبارت سادهتر EMET یک لایه امنیتی را پیرامون سیستمعامل قرار میدهد .

برایان کربس، از کارشناسان امنیتی در همین ارتباط گفته است : «من معتقد هستم این اکسپلویت واقعی است. اما یک لایه واسط در این بین وجود دارد . به دلیل اینکه این آسیبپذیری روز صفر تنها باعث به وجود آمدن یک وضعیت ناپایدار در سطح مجوزها در ماشین مقصد میشود. در نتیجه برای آنکه این آسیبپذیری به یک تهدید بالقوه تبدیل شود، مهاجم نیازمند آسیبپذیریهای دیگری است که با این آسیبپذیری هماهنگ شوند تا یک خطر جدی را به وجود آورند .»

کربس در بخشی از صحبتهای خود یادآور شده است: «برای من بسیار جالب است که مشاهده میکنیم مجرمان سایبری چگونه این توانایی را دارند تا آسیبپذیریهای روز صفر را بهطور مستقیم و به قیمت بالایی نسبت به برنامه تشویقی مایکروسافت به فروش برسانند . مایکروسافت یک برنامه تشویقی اشکال زادیی دارد که بهطور منظم به محققان امنیتی که توانایی کشف آسیبپذیریها و گزارش آنها را داشته باشند مبالغی را اهدا میکند . مایکروسافت به تازگی رقم تشویقی خود را به 100 هزار دلار در ارتباط با اکسپلویتهای روز صفر افزایش داده است، برنامهای که EMET را نیز پوشش میدهد.»

در هر حالت متاعی همچون آسیبپذیری روز صفر در حال تبدیل شدن به روند نگران کننده در سراسر جهان شده است. بهطوری که امنیت و حریم دیجیتالی کاربران را در معرض یک تهدید جدی قرار داده است .

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
21:13 - 30/03/1395
برچسب:
ویندوز - امنیت - اکسپلویت - آسیبپذیری - روز صِفر - EMET - رخنه

□□□□□ منبع :https://www.shabakeh-mag.com/security/3535