خبرنامه‌ی تخصصی امنیت

هفته‌نامه‌ی شماره ۲، آذر ۹۹، سال اول
مرکزتخصصی آپا ـ دانشگاه ارومیه

آنچه در این شماره ارائه شده:

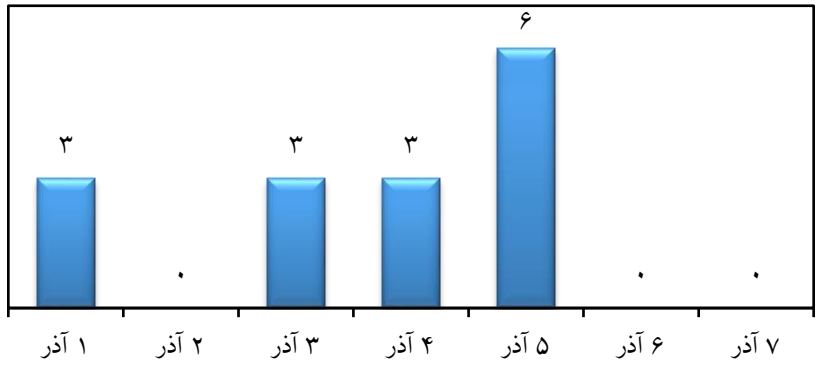
- مروری بر آسیب‌پذیری‌های مهم هفته
- آسیب‌پذیری‌های مهم در محصولات شرکت‌های VMware، اینتل و لینوکس
- خبرهای مهم امنیتی این هفته

بسم الله الرحمن الرحيم

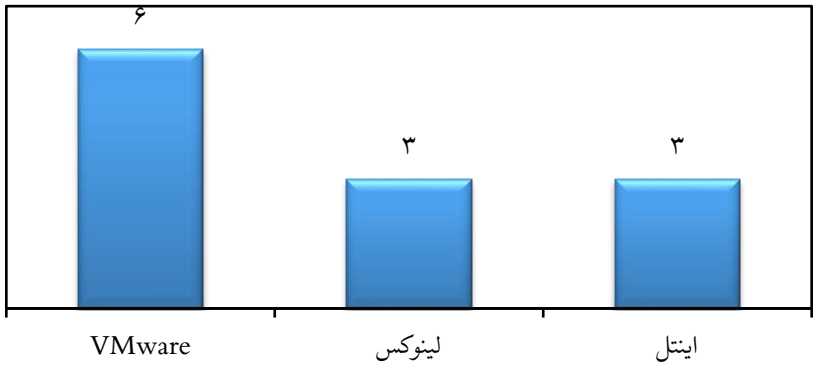
مروری بر آسیب‌پذیری‌های مهم هفته‌ی اول آذر سال ۹۹

در هفته‌ای که گذشت، چندین آسیب‌پذیری بحرانی و مشکل‌ساز در محصولات شرکت‌های مختلف شناسایی شدند. در میان شرکت‌های مختلف، VMware بیشترین محصولات آسیب‌پذیر را به خود اختصاص داده است. همچنین، بیشتر آسیب‌پذیری‌ها از نوع ارتقای امتیاز و خرابی حافظه هستند. در ادامه، آمار و اطلاعات مربوط به این آسیب‌پذیری‌ها ارائه شده است.

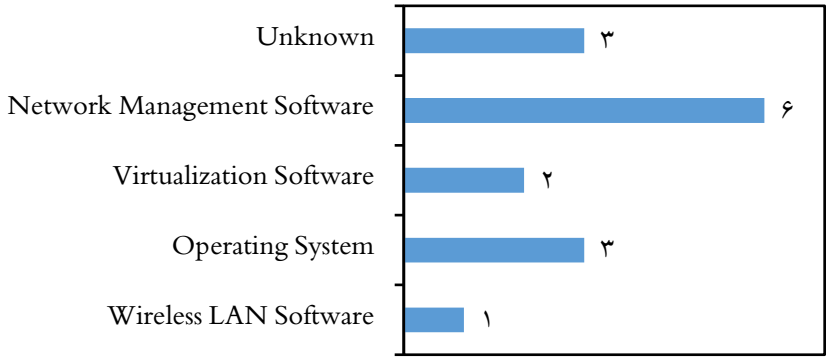
تعداد آسیب‌پذیری‌ها به تفکیک روزهای هفته



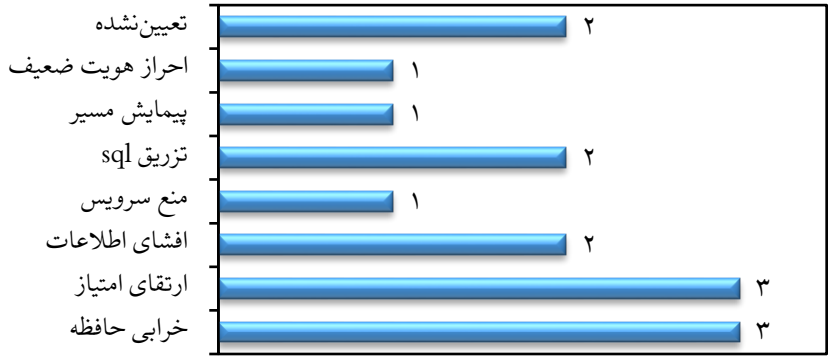
تعداد آسیب‌پذیری‌ها به تفکیک شرکت‌های سازنده



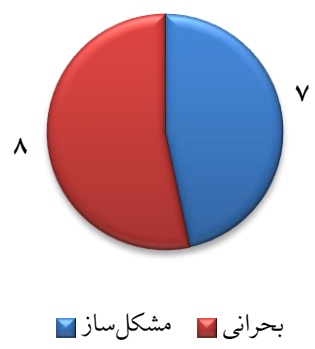
انواع محصولات آسیب‌پذیر



نوع آسیب‌پذیری‌ها



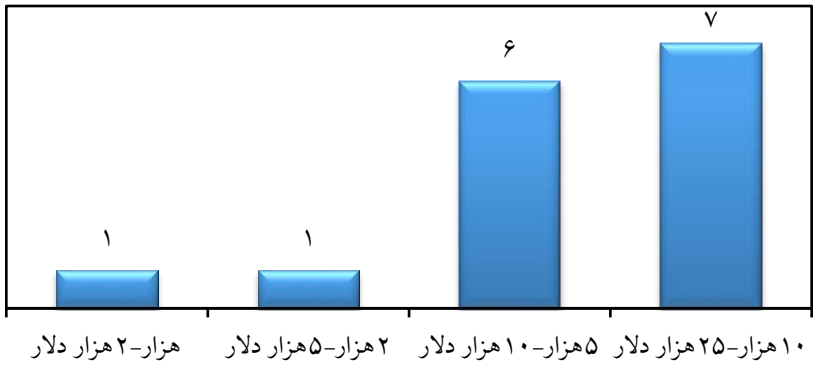
سطح خطر آسیب‌پذیری‌ها



بردار دسترسی آسیب‌پذیری‌ها

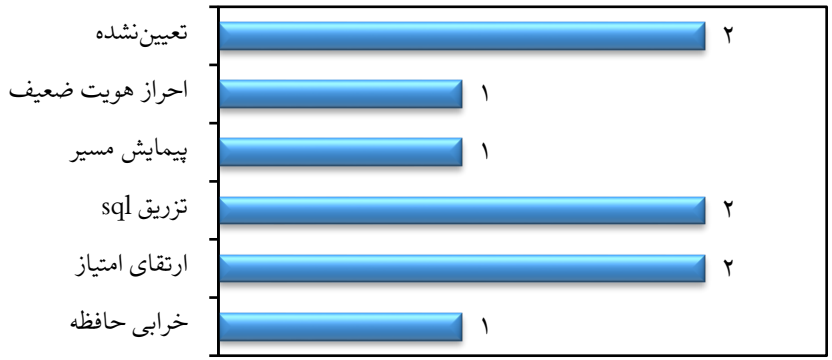
نیاز به احراز هویت برای بهره‌برداری از آسیب‌پذیری‌ها

ارزش روز صفر آسیب‌پذیری‌ها

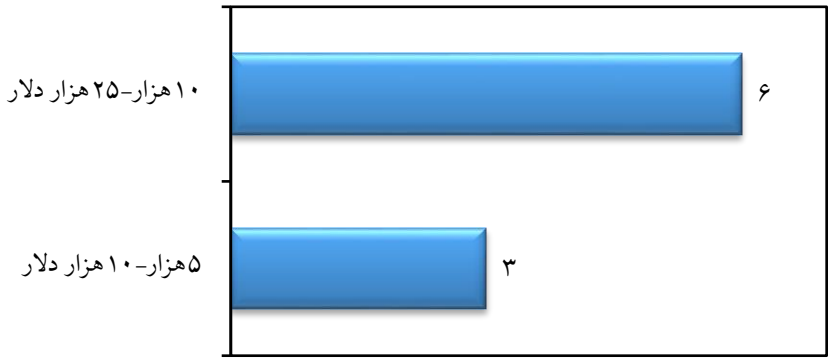


آسیب‌پذیری‌های شناسایی‌شده در محصولات شرکت VMware

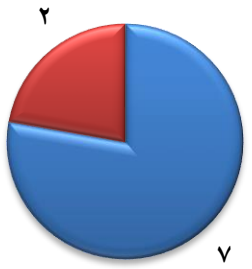
نوع آسیب‌پذیری‌ها



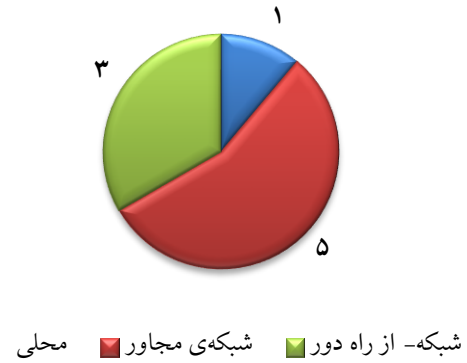
ارزش روز صفر آسیب‌پذیری‌ها



سطح خطر آسیب‌پذیری‌ها



بردار دسترسی آسیب‌پذیری‌ها



نیاز به احراز هویت برای بهره‌برداری از آسیب‌پذیری‌ها

آسیب‌پذیری بحرانی CVE-2020-4004 در VMware Workstation، ESXi و Fusion

- این اشکال امنیتی برخی توابع ناشناخته در مؤلفه‌ی XHCI USB Controller را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به خرابی حافظه می‌شود. بردار حمله به‌صورت محلی است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت چند مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری از طریق به‌روزرسانی محصول وصله می‌شود.

آسیب‌پذیری بحرانی CVE-2020-4005 در VMware ESXi

- این اشکال امنیتی یک بخش ناشناخته از مؤلفه‌ی System Call Handler را تحت تأثیر قرار می‌دهد. نوع آسیب‌پذیری مشخص نیست. بردار حمله به‌صورت شبکه و از راه دور است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقای محصول به نسخه‌های ۶/۵، ۶/۷ یا ۷/۰ وصله می‌شود.

آسیب‌پذیری بحرانی CVE-2020-4006 در VMware Identity Manager ،Connector Workspace One Access ،Access و Identity Manager Connector

- این اشکال امنیتی برخی از پردازش‌های ناشناخته را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به ارتقای امتیاز می‌شود. بردار حمله به‌صورت شبکه‌ی مجاور است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. هیچ اطلاعاتی در مورد اقدامات متقابل احتمالی در برابر این آسیب‌پذیری منتشر نشده و در حال حاضر، جایگزینی شیء (object) آسیب‌دیده با یک محصول جایگزین پیشنهاد می‌شود.

آسیب‌پذیری بحرانی CVE-2020-3984 در VMware SD-WAN Orchestrator

- این اشکال امنیتی یک کد ناشناخته را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به تزریق sql می‌شود. مهاجم می‌تواند با تزریق و یا تغییر عبارت‌های SQL موجود، پایگاه داده را تحت تأثیر قرار دهد. بردار حمله به‌صورت شبکه و از راه دور است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقای محصول به نسخه‌های 3.3.2P3 و 3.4.4 وصله می‌شود.

آسیب‌پذیری بحرانی CVE-2020-3985 در VMware SD-WAN Orchestrator

- این اشکال امنیتی یک بلوک کد ناشناخته در مؤلفه‌ی API را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به ارتقای امتیاز می‌شود. بردار حمله به‌صورت شبکه و از راه دور است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقای محصول به نسخه‌های 3.3.2P3 و 3.4.4 وصله می‌شود.

آسیب‌پذیری بحرانی CVE-2020-4000 در VMware SD-WAN Orchestrator

- این اشکال امنیتی برخی از پردازش‌های ناشناخته را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به پیمایش مسیر (directory traversal) می‌شود. بردار حمله به‌صورت شبکه‌ی مجاور است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقای محصول به نسخه‌های 3.3.2P3، 3.4.4 و 4.0.1 وصله می‌شود.

آسیب‌پذیری مشکل‌ساز CVE-2020-4001 در VMware SD-WAN Orchestrator

• این اشکال امنیتی یک تابع ناشناخته را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به احراز هویت ضعیف می‌شود. بردار حمله به‌صورت شبکه‌ی مجاور است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت نیاز نیست. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است.

آسیب‌پذیری مشکل‌ساز CVE-2020-4002 در VMware SD-WAN Orchestrator

• این اشکال امنیتی یک تابع ناشناخته در مؤلفه‌ی System Parameter Handler را تحت تأثیر قرار می‌دهد. نوع آسیب‌پذیری مشخص نیست. بردار حمله به‌صورت شبکه‌ی مجاور است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقای محصول به نسخه‌های 3.3.2P3، 3.4.4 و 4.0.1 وصله می‌شود.

آسیب‌پذیری بحرانی CVE-2020-4003 در VMware SD-WAN Orchestrator

• این اشکال امنیتی برخی توابع ناشناخته را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به تزریق sql می‌شود. مهاجم می‌تواند با تزریق و یا تغییر عبارت‌های SQL موجود، تبادل پایگاه داده را تحت تأثیر قرار دهد. بردار حمله به‌صورت شبکه‌ی مجاور است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقای محصول به نسخه‌های 3.3.2P3، 3.4.4 و 4.0.1 وصله می‌شود.

آسیب‌پذیری‌های شناسایی‌شده در محصولات شرکت اینتل

آسیب‌پذیری مشکل‌ساز CVE-2020-0569 در PROSet و Wireless WiFi اینتل

• این اشکال امنیتی یک تابع ناشناخته را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به خرابی حافظه می‌شود. بردار حمله به‌صورت محلی است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. هیچ اطلاعاتی در مورد اقدامات متقابل احتمالی در برابر این آسیب‌پذیری منتشر نشده و در حال حاضر، جایگزینی شیء (object) آسیب‌دیده با یک محصول جایگزین پیشنهاد می‌شود.

آسیب‌پذیری بحرانی CVE-2020-12351 در BlueZ اینتل

• این اشکال امنیتی برخی توابع ناشناخته را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به ارتقای امتیاز می‌شود. بردار حمله به‌صورت شبکه‌ی مجاور بوده و برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت نیاز نیست. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با اعمال وصله رفع می‌شود.

آسیب‌پذیری مشکل‌ساز CVE-2020-12352 در BlueZ اینتل

• این اشکال امنیتی یک بخش ناشناخته را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به افشای اطلاعات می‌شود. بردار حمله به‌صورت شبکه‌ی مجاور بوده و برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت نیاز نیست. جزئیات فنی این اشکال ناشناخته بوده و بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با اعمال وصله رفع می‌شود.

آسیب‌پذیری‌های شناسایی‌شده در لینوکس

آسیب‌پذیری مشکل‌ساز CVE-2020-28974 در Kernel لینوکس

• این اشکال امنیتی تابع KD_FONT_OP_COPY در فایل drivers/tty/vt/vt.c در مؤلفه‌ی fbcon را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به افشای اطلاعات می‌شود. بردار حمله به‌صورت محلی است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال مشخص بوده، ولی بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقا به نسخه‌ی ۵/۹/۷ وصله می‌شود.

آسیب‌پذیری مشکل‌ساز CVE-2020-15436 در Kernel لینوکس

• این اشکال امنیتی یک کد ناشناخته از فایل fs/block_dev.c در مؤلفه‌ی Error Field Handler را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به خراب حافظه می‌شود. بردار حمله به‌صورت محلی است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال مشخص بوده، ولی بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقا به نسخه‌ی ۵/۸ وصله می‌شود.

آسیب‌پذیری مشکل‌ساز CVE-2020-15437 در Kernel لینوکس

• این اشکال امنیتی تابع serial8250_isa_init_ports در فایل drivers/tty/serial/8250/8250_core.c را تحت تأثیر قرار داده و با دستکاری از طریق ورودی ناشناخته، منجر به منع سرویس می‌شود. بردار حمله به‌صورت محلی است و به نظر می‌رسد بهره‌برداری از آن آسان باشد. برای بهره‌برداری از این آسیب‌پذیری، به احراز هویت تک مرحله‌ای نیاز است. جزئیات فنی این اشکال مشخص بوده، ولی بهره‌برداری از آن عمومی نشده است. این آسیب‌پذیری با ارتقا به نسخه‌ی ۵/۸ وصله می‌شود.

خبرهای مهم امنیتی در هفته‌ی اول آذر ماه سال ۹۹

۱ آذر

شنود کاربران قبل از پاسخ به تماس در برنامه‌ی فیس‌بوک مسنجر

شرکت فیس‌بوک، یک آسیب‌پذیری امنیتی موجود در برنامه‌ی مسنجر خود برای سیستم عامل اندروید را وصله کرد. این اشکال به مهاجم راه دور اجازه می‌دهد تا با اهداف تماس گرفته و قبل از این‌که آنها تماس صوتی را پاسخ دهند، به صدای آنها گوش کند. طبق گزارش‌ها، این آسیب‌پذیری نسخه‌ی ۲۸۴/۰/۰/۱۶/۱۱۹ (و قبل از آن) برنامه‌ی فیس‌بوک مسنجر را در سیستم عامل اندروید تحت تأثیر قرار می‌دهد.

۴ آذر

هدف قرارگرفتن سرورهای لینوکس توسط بات‌نت Stantinko

بات‌نت تبلیغاتی و استخراج‌کننده‌ی ارز دیجیتال Stantinko که از سال ۲۰۱۲ میلادی کاربران روسیه، اوکراین، بلاروس و قزاقستان را هدف قرار می‌دهد، اکنون برای جلوگیری از شناسایی خود، سرورهای لینوکس را هدف قرار داده است. به گفته‌ی محققان، نسخه‌ی جدید این تروجان در قالب HTTPd، برنامه‌ای که معمولاً در سرورهای لینوکس مورد استفاده قرار می‌گیرد، ظاهر می‌شود.

۴ آذر

دورزدن احراز هویت دو عاملی در نرم‌افزار cPanel & WHM

ارائه‌دهنده‌ی ابزارهای مدیریت میزبانی وب cPanel، از وصله‌ی یک آسیب‌پذیری امنیتی که امکان دورزدن قابلیت احراز هویت دو عاملی در یک حساب را برای مهاجم راه دور فراهم می‌کند، خبر داد. این آسیب‌پذیری که با شناسه‌ی SEC-575 ردیابی می‌شود، توسط این شرکت در نسخه‌های ۱۱/۹۲/۰/۲، ۱۱/۹۰/۰/۱۷ و ۱۱/۸۶/۰/۳۲ نرم‌افزار cPanel & WHM وصله شده است.