مهمترین آسیب‌پذیری‌های روترهای میکروتیک

جمع‌آوری: آرین فقیراللهی

- **مقدمه**

میکروتیک یک شرکت در لتونی است که در سال ۱۹۹۶ برای توسعه روترها و سیستم‌های بی‌سیم ISP تأسیس شد. مهمترین محصول این شرکت سیستم‌عامل میکروتیک است. سیستم‌عامل میکروتیک مسیریابی است که با استفاده از هسته لینوکس توسعه داده شده است. سیستم‌عامل میکروتیک علاوه‌بر قابلیت نصب بر روی رایانه‌های خانگی، به صورت بسته نرم‌افزاری-سخت‌افزاری نیز ارائه شده است. این سیستم عامل و دیگر تجهیزات سخت افزاری و نرم افزاری این شرکت همانند بسیاری از تجهیزات رایانه‌ای، دارای آسیب‌پذیری‌های گوناگونی هستند. در ادامه این گزارش به ۲۶ مورد از مهمترین آسیب‌پذیری‌های عمومی کشف شده در محصولات میکروتیک پرداخته می‌شود. بسیاری از این آسیب‌پذیری‌های مهم در سال‌های اخیر (۲۰۱۵ به بعد) کشف شده‌اند. این بدان معنا است که میکروتیک در حال تصاحب سهم بیشتری از بازار تجهیزات ارتباطی و مخابراتی است، امری که موجب می شود به امنیت محصولات و تجهیزات این شرکت توجه بیشتری شود. این لیست براساس میزان درجه حساسیت آسیب‌پذیری بر اساس معیار CVSS مرتب شده است.

- **لیست آسیب‌پذیری‌ها**

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#1	CVE-2018-7445	Exec Code Overflow	2018-04-24	10.0/10	Remote
هنگام پردازش پیام‌های درخواست جلسه NetBIOS، یک سرریز بافر در سرویس MikroTik Router OS SMB کشف شده است. مهاجمان راه دور با دسترسی به سرویس می‌توانند از این آسیب‌پذیری سوءاستفاده کرده و اجرای کد را در سیستم به دست آورند. سرریز قبل از احراز هویت اتفاق می‌افتد، بنابراین ممکن است یک مهاجم راه دور احراز هویت نشده از آن سوءاستفاده کند. همه معماری‌ها و همه دستگاه‌هایی که Router OS قبل از نسخه‌های ۶.۴۲/۶.۴۱.۳ ۲۷rc دارند، آسیب‌پذیر هستند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#2	CVE-2018-1156	Exec Code Overflow	2020-08-24	9.0/10	Remote
MikroTik Router OS قبل از ۶.۴۲.۷ و ۶.۴۰.۹ در برابر سرریز بافر پشته از طریق رابط ارتقا لایسنس آسیب‌پذیر است. این آسیب‌پذیری از نظر می‌تواند به مهاجم تأیید شده از راه دور اجازه دهد تا کد دلخواه را روی سیستم اجرا کند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#3	CVE-2019-3977	-	2019-11-01	8.5/10	Remote
RouterOS ۶.۴۵.۶ ، هنگام استفاده از ویژگی ارتقای خودکار، بسته‌های ارتقا را از منبعی تایید نشده دانلود می‌کنند. بنابراین، یک مهاجم از راه دور می‌تواند روتر را فریب دهد تا به نسخه قدیمی‌تر RouterOS ۶.۴۴.۵ تغییر یابد و قابلیت بازنشانی همه نام‌های کاربری و رمزهای عبور سیستم را پیدا کند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#4	CVE-2021-27221	-	2021-03-26	8.5/10	Remote

MikroTik RouterOS ۶.۴۷.۹ به کاربران FTP احراز هویت شده از راه دور اجازه می‌دهد تا فایل‌های دلخواه rsc. را از طریق فرمان export ایجاد یا بازنویسی کنند. البته این آسیب‌پذیری مورد مناقشه است و موضع شرکت این است که این رفتار مورد نظر به دلیل نحوه عملکرد خط‌مشی‌های کاربر است.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#5	CVE-2017-7285	-	2017-04-10	7.8/10	Remote

یک آسیب‌پذیری در پشته شبکه MikroTik نسخه ۶.۳۸.۵ منتشر شده در ۲۰۱۷/۰۳/۰۹ می‌تواند به یک مهاجم راه دور تأیید نشده اجازه دهد تا تمام CPU موجود را از طریق سیل بسته‌های TCP RST تخلیه کند و از پذیرش اتصالات TCP جدید توسط روتر آسیب‌دیده جلوگیری کند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#6	CVE-2017-8338	-	2019-10-03	7.8/10	Remote

یک آسیب‌پذیری در MikroTik نسخه ۶.۳۸.۵ می‌تواند به یک مهاجم راه دور تأیید نشده اجازه دهد تا تمام CPU موجود را از طریق سیل بسته‌های UDP در پورت ۵۰۰ (که برای L2TP از طریق IPsec استفاده می‌شود) تخلیه کند و از پذیرش اتصالات جدید توسط روتر آسیب‌دیده جلوگیری کند. همه دستگاه ها از روتر جدا می شوند و همه گزارش ها به طور خودکار حذف می شوند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#7	CVE-2020-22845	DoS Overflow	2022-03-08	7.8/10	Remote

یک سرریز بافر در Mikrotik Router OS ۶.۴۷ به مهاجمان احراز هویت نشده اجازه می‌دهد تا از طریق درخواست‌های FTP ساخته شده، باعث انکار سرویس (DOS) شوند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#8	CVE-2019-3943	Dir. Trav	2019-12-17	7.5/10	Remote

MikroTik RouterOS نسخه‌های پایدار ۶.۴۳.۱۲ و پایین‌تر، ۶.۴۲.۱۲ و پایین‌تر، و ۶.۴۴beta۷۵ و پایین‌تر در برابر پیمایش دایرکتوری احراز هویت شده از راه دور از طریق رابط‌های HTTP یا Winbox آسیب‌پذیر هستند. یک مهاجم احراز هویت شده و از راه دور می‌تواند از این آسیب‌پذیری برای خواندن و نوشتن فایل‌های خارج از پوشه سندباکس (rw/disk) استفاده کند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#9	CVE-2018-5951	-	2020-03-04	7.1/10	Remote

ایجاد بسته‌ای که اندازه آن ۱ بایت است و ارسال آن به آدرس ۶IPv جعبه RouterOS با IP Protocol ۹۷ باعث راه‌اندازی مجدد RouterOS می‌شود. تمام نسخه‌های RouterOS که از ۶EoIPv پشتیبانی می‌کنند در برابر این حمله آسیب‌پذیر هستند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#10	CVE-2015-2350	CSRF	2015-09-24	6.8/10	Remote

آسیب‌پذیری جعل درخواست‌های متقابل (CSRF) در MikroTik RouterOS ۵.۰ و نسخه‌های قبلی به مهاجمان راه دور اجازه می‌دهد تا احراز هویت مدیران را برای درخواست‌هایی که رمز عبور مدیر را از طریق درخواست در صفحه وضعیت به cfg تغییر می‌دهند، بربایند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#11	CVE-2018-1157	-	2019-07-23	6.8/10	Remote

Mikrotik RouterOS قبل از ۶.۴۲.۷ و ۶.۴۰.۹ در برابر آسیب‌پذیری memory exhaustion آسیب پذیر است. یک مهاجم از راه دور تأیید شده می‌تواند سرور HTTP را خراب کند و در برخی شرایط سیستم را از طریق یک درخواست HTTP POST دستکاری شده راه‌اندازی مجدد کند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#12	CVE-2018-10066	-	2018-05-17	6.8/10	Remote

عدم تأیید گواهی سرور OpenVPN به یک مهاجم تأیید نشده از راه دور که قادر به رهگیری ترافیک مشتری است اجازه می‌دهد تا به عنوان یک سرور OpenVPN مخرب عمل کند. این ممکن است به مهاجم اجازه دهد تا به شبکه داخلی مشتری دسترسی پیدا کند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#13	CVE-2019-13954	-	2020-08-24	6.8/10	Remote

Mikrotik RouterOS قبل از ۶.۴۴.۵ در برابر تخریب حافظه آسیب‌پذیر است. با ارسال یک درخواست HTTP دستکاری شده، یک مهاجم از راه دور تأیید شده می‌تواند سرور HTTP را خراب کند و در برخی شرایط سیستم را راه اندازی مجدد کند. البته کد مخرب را نمی‌توان تزریق کرد.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#14	CVE-2020-20221	Dos	2021-07-30	6.8/10	Remote

Mikrotik RouterOs قبل از ۶.۴۴.۶ دارای آسیب‌پذیری مصرف منابع کنترل نشده در فرآیند nova/bin/cerm است. یک مهاجم از راه دور تأیید شده می تواند به دلیل بارگذاری بیش از حد CPU سیستم باعث انکار سرویس شود.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#15	CVE-2021-41987	Exec Code Overflow	2022-03-29	6.8/10	Remote

در سرور SCEP RouterOS در برخی از محصولات Mikrotik، یک مهاجم می‌تواند یک سرریز بافر مبتنی بر پشته ایجاد کند که منجر به اجرای کد از راه دور می‌شود. مهاجم باید مقدار scep_server_name را بداند. این مورد روی RouterOS ۶.۴۶.۸، ۶.۴۷.۹ و ۶.۴۷.۱۰ تأثیر می‌گذارد.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#16	CVE-2019-3976	Dir. Trav	2021-11-03	6.5/10	Remote

RouterOS 6.44.5، RouterOS 6.45.6 Stable و پایین‌تر در برابر آسیب‌پذیری ایجاد دایرکتوری دلخواه از طریق فیلد نام بسته ارتقاء، آسیب‌پذیر هستند. اگر یک کاربر احراز هویت شده یک بسته مخرب را نصب کند، می‌توان یک دایرکتوری ایجاد کرد و پوسته توسعه‌دهنده را فعال کرد.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#17	CVE-2008-6976	-	2022-02-09	6.4/10	Remote

MikroTik RouterOS 3.x تا ۳.۱۳ و ۲.x تا ۲.۹.۵۱ به مهاجمان راه دور اجازه می‌دهد تا تنظیمات سیستم مدیریت شبکه (NMS) را از طریق یک درخواست تنظیم SNMP دستکاری شده تغییر دهند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#18	CVE-2012-6050	Dos and others	2017-08-29	6.4/10	Remote

MikroTik سرویس winbox در MikroTik RouterOS ۵.۱۵ و نسخه‌های قبلی به مهاجمان از راه دور اجازه می‌دهد تا باعث انکار سرویس، مصرف CPU، خواندن نسخه روتر و احتمالاً تأثیرات دیگری از طریق درخواست بارگیری DLL یا افزونه‌های روتر شوند.

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#19	CVE-2018-14847	Dir. Trav.	2019-03-07	6.4/10	Remote
MikroTik RouterOS از طریق نسخه ۶.۴۲ به مهاجمان راه دور تأیید نشده اجازه می‌دهد تا فایل‌های دلخواه را بخوانند و مهاجمان تأیید شده از راه دور فایل‌های دلخواه را به دلیل آسیب‌پذیری پیمایش دایرکتوری در رابط WinBox بنویسند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#20	CVE-2019-15055	Dir. Trav.	2020-10-06	5.5/10	Remote
MikroTik RouterOS در نسخه‌های ۶.۴۴.۵ و ۶.۴۵.۱ تا ۶.۴۵.۳ نام دیسک را به درستی مدیریت نمی‌کند که به کاربران تأیید شده اجازه می‌دهد فایل‌های دلخواه را حذف کنند. مهاجمان می‌توانند از این آسیب‌پذیری برای بازنشانی فضای ذخیره‌سازی اعتبار سوءاستفاده کنند، که به آنها اجازه می‌دهد به عنوان یک سرپرست بدون احراز هویت به رابط مدیریت دسترسی داشته باشند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#21	CVE-2019-3924	Bypass	2019-10-09	5.0/10	Remote
MikroTik RouterOS قبل از ۶.۴۳.۱۲ (پایدار) و ۶.۴۲.۱۲ در برابر یک آسیب‌پذیری واسطه آسیب‌پذیر است. این نرم افزار درخواست‌های شبکه تعریف شده توسط کاربر را برای مشتریان WAN و LAN اجرا می‌کند. یک مهاجم تایید نشده از راه دور می‌تواند از این آسیب‌پذیری برای دور زدن فایروال روتر یا برای فعالیت‌های عمومی اسکن شبکه استفاده کند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#22	CVE-2019-3978	-	2019-11-01	5.0/10	Remote
RouterOS نسخه ۶.۴۵.۶، ۶.۴۴.۵ و پایین‌تر به مهاجمان احراز هویت نشده از راه دور اجازه می‌دهد تا درخواست‌های DNS را از طریق پورت ۸۲۹۱ راه‌اندازی کنند. درخواست‌ها از روتر به سروری به انتخاب مهاجم ارسال می‌شوند. پاسخ‌های DNS توسط روتر ذخیره می‌شوند و به طور بالقوه منجر به آلوده شدن حافظه پنهان می‌شوند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#23	CVE-2019-3979	-	2021-07-21	5.0/10	Remote
RouterOS نسخه ۶.۴۵.۶، ۶.۴۴.۵ و پایین‌تر در برابر حمله داده‌های نامربوط به DNS آسیب‌پذیر هستند. روتر تمام رکوردهای A را به حافظه نهان DNS خود اضافه می‌کند، حتی زمانی که رکوردها به دامنه‌ای که درخواست شده ارتباطی نداشته باشند. بنابراین، یک سرور DNS کنترل شده توسط مهاجم از راه دور می‌تواند کش DNS روتر را از طریق پاسخ‌های مخرب با سوابق اضافی و غیر واقعی آلوده کند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#24	CVE-2019-16160	-	2021-07-21	5.0/10	Remote
زیر جریان عدد صحیح در سرور MikroTik RouterOS SMB قبل از ۶.۴۵.۵ به مهاجمان احراز هویت نشده از راه دور اجازه می‌دهد تا سرویس را خراب کنند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#25	CVE-2020-11881	-	2020-09-18	5.0/10	Remote
یک خطای فهرست آرایه در MikroTik RouterOS ۶.۴۱.۳ تا ۶.۴۶.۵، و ۷.x تا ۷.۰ Beta، به مهاجم راه دور تأیید نشده اجازه می‌دهد تا سرور SMB را از طریق بسته‌های درخواست تنظیم تغییر یافته، با نام SUP-۱۲۹۶۴، خراب کند.					

شماره	شناسه آسیب‌پذیری	نوع آسیب‌پذیری	زمان انتشار	امتیاز	نوع دسترسی
#26	CVE-2020-22844	DoS, buffer Overflow	2022-03-08	5.0/10	Remote
سرریز بافر در Mikrotik RouterOS ۶.۴۷ به مهاجمان احراز هویت نشده اجازه می‌دهد تا از طریق درخواست‌های SMB ساخته شده، باعث انکار سرویس (DOS) شوند.					

- **جمع‌بندی**

این گزارش مروری بر مهمترین آسیب‌پذیری‌های کشف شده در سیستم‌عامل میکروتیک بوده است. این آسیب‌پذیری‌ها فارغ از زمان انتشار، درجه حساسیت بیش از ۵ را بر طبق معیار CVSS به خود اختصاص داده‌اند. همانطور که در ابتدا اشاره شد، افزایش تعداد آن‌ها در سال‌های اخیر حاکی از افزایش تقاضا برای تجهیزات میکروتیک است، امری که موضوع امنیت آن را بیش از پیش موردتوجه قرار می‌دهد و نشان‌دهنده رابطه مستقیم میان افزایش تقاضا برای تجهیزات و افزایش علاقه‌مندی برای نا امن کردن تجهیزات پر کاربرد است. یکی از راه‌حل‌های اساسی و همیشگی برای مقابله با این آسیب‌پذیری‌ها به‌روزرسانی‌های منظم، اعمال وصله‌های منتشر شده و پیکربندی صحیح است که با این اعمال به ظاهر ساده می‌توان بسیاری از این آسیب‌پذیری‌ها را رفع و ارتباطات امن‌تری برای کاربران فراهم کرد.

منبع:

https://www.cvedetails.com/vulnerability-list.php?vendor_id=12508&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=3&trc=65&sha=ceae065bce8f7e1c8a98de53f22abf92fae90a9f