باسمه تعالی

عنوان مستند

آسیب پذیریAuthenticated Remote File Disclosure در مودم روترهای وایرلسNetgear

فهرست مطالب

۱ چکیده

مدل‌های متنوعی از مودم روترهای وایرلس ساخت شرکت Netgear دارای آسیب پذیری Authenticated Remote File Disclosure می‌باشند که این آسیب پذیری باعث افشاسازی اطلاعات مربوط به فایل‌های اساسی مودم روتر و دستکاری فایل‌های صفحه‌ی ادمین مودم خواهد شد. این آسیب‌پذیری دسترسی به یک فایل خاص همچون XML یا هر فایل دیگری را با تایپ یک URL خاص میسر می‌سازد که در قسمت‌های بعد بصورت کامل بررسی خواهند گردید.

۲ محصولات تحت تاثیر

نتایج اجرای حمله بر روی مدل‌های WNR۵۰۰، WNR۶۱۲v۳، JNR۱۰۱۰، JNR۲۰۱۰ و به ترتیب با ورژن‌های سفت افزاری ۱,۰,۷,۲، ۱,۰,۰,۹، ۱,۰,۰,۳۲ و ۱,۰,۰,۲۰ تست شده و دارای آسیب پذیری می‌باشند.

۳ تاثیر آسیب پذیری

مهاجم تنها با کمترین امکانات و تنها استفاده از یک سیستم می‌تواند به مودم روترهای مورد استفاده در سازمانها یا ارگانها حمله نموده و با اجرای دستورات از راه دور باعث از کار انداختن آنها و دخیره سازی و افشای اطلاعات مودم روتر و عدم ارائه‌ی سرویس‌ها به کاربران شود. تاثیر این آسیب پذیری بر تمامی کاربران خانگی و همچنین ارگانها و یا سازمانهایی که از این مدل مودم روترها بهره می‌برند، هویداست. به سازمان‌ها توصیه می‌شود تاثیر این آسیب‌پذیری‌ها را بر اساس محیط عملیاتی، معماری و پیاده سازی محصول شان ارزیابی کنند.

۴ مشخصه های آسیب پذیری

در این قسمت به مرور کامل مشخصه‌های آسیب پذیری و ذکر کامل سناریوی حمله به بحث مفصلاً پرداخته خواهد شد. در بخش‌های آتی در این خصوص توضیح داده می‌شود.

۴-۱ مروری بر آسیب‌پذیری

آسیب‌پذیری مشاهده شده در این چند مدل از مودم روترهای وایرلس تماما از راه دور قابل انجام است. مهاجم بعد از بدست آوردن یوزر و پسورد و تنها با تایپ یک لینک یا آدرس خاص اقدام به افشا سازی، دانلود و یا تغییر اطلاعات حساس مودم روتر می‌نماید.

۴-۱-۱ مسائل دور زدن احراز هویت

در این حمله با اجرای دستورات از راه دور و از طریق وب می‌توان باعث نفوذ و دستکاری‌های بخصوصی در فایلها و اطلاعات حساس مودم روتر وایرلس انجام داده و موجب دورزدن پروسه‌ی احراز هویت در دستیابی به اطلاعات صفحه‌ی تنظیمات مودم شد.

۴-۲ جزییات آسیب پذیری

در این بخش به معرفی جزییات مربوط به آسیب‌پذیری و تمامی مسایل و راهکارهای ایجاد آسیب‌پذیری پرداخته خواهد شد. در این نوع از حمله اطلاعات خاص در مورد سیستم مودم روتر از جمله مدل، شماره نسخه و سازنده، پسورد وایرلس و صفحه‌ی ادمین مودم، SSID و غیره به دست آورده می‌شود. اطلاعات به دست آمده همچنین ممکن است شامل محل فایل های پشتیبان گیری و یا فایل های موقت باشد.

۴-۲-۱ قابلیت بهره برداری

بهره برداری از این آسیب پذیری می‌تواند کاملا از راه دور و از طریق وب انجام گیرد و باعث دسترسی به اطلاعات و نقض شدن محرمانگی فایل‌ها و اطلاعات حساس مودم شود.

۴-۲-۲ بهره برداری موجود

تا کنون سوء استفاده‌ی عمومی که در مورد این آسیب پذیری‌ها باشد، منتشر نشده است. اما به راحتی و با کمترین امکانات و تنها با یک سیستم خانگی ساده و یک اینترنت معمولی می‌توان بصورت کامل از این حملات - حتی در سطح کلان- سوء استفاده نمود.

۴-۲-۳ سطح آسیب پذیری

یک مهاجم با مهارت‌های تقریبا متوسط، می‌تواند از این آسیب‌پذیری سوء استفاده کند. پس سطح این آسیب‌پذیری در محدوده‌ی متوسط یا نیمه بحرانی است.

۵ اقدامات جهت کاهش شدت آسیب پذیری

از جمله راهکارهای مقابله با این نوع حمله ها، آپدیت سفت افزار مودم به نسخه‌های بالاتر و در نتیجه رفع باگ‌ها و آسیب‌پذیری‌های مشروح، برای استفاده کنندگان می‌باشد.

۶ جمع بندی و نتیجه‌گیری

در قسمت‌های پیشین در خصوص آسیب‌پذیری‌های مودم روترهای وایرلس ساخت شرکت Netgear دارای آسیب پذیریAuthenticated Remote File Disclosure که باعث افشاسازی اطلاعات مربوط به فایل‌های اساسی مودم روتر و دستکاری فایل‌های صفحه‌ی ادمین مودم خواهد شد به تفصیل به بحث پرداخته شد. با استفاده از این لینک‌ها می‌توان با داشتن ورژن آسیب پذیر سفت افزار مودم اقدام به نفوذ و نقض احراز هویت و سرقت اطلاعات و خصوصا پسورد وایرلس مودم روتر نمود. با توجه به مستندات موجود مدل فوق در کشورمان ایران نیز بهره‌برداری و استفاده می‌شود.

۷ منابع

[۱]https://www.ibm.com/support/knowledgecenter/en/SSB۲MG_۴,۶,۰/com.ibm.ips.doc/concepts/wap_information_disclosure.htm

[۲] https://www.exploit-db.com/exploits/۴۰۷۳۷/

[۳] https://www.exploit-db.com/exploits/۴۰۷۳۶/

[۴] https://www.iranonymous.org/

[۵] https://www.ethical-hacker.org/