کشف چندین آسیب پذیری مهم

و درب پشتی سخت افزاری در برخی هاردهای NAS شرکت Western Digital

تهیه کننده : حامد زندی

فهرست مطالب

۱) مقدمه

محققین امنیتی موفق شدند چند آسیب پذیری مهم و یک درب پشتی(بک در) سخت افزاری مخفی را در هاردهای NAS از نوع My Cloud شرکت Western Digital شناسایی کنند. این نوع هاردهای متصل به شبکه برای نگهداری فایل ها و نسخه های پشتیبان به صورت فردی و سازمانی کاربرد دارد. علاوه بر اشتراک گذاری محلی فایل ها، قابلیت "ابر اختصاصی" موجود در این تجهیزات اماکن دسترسی به فایل ها را از هر نقطه می دهد. به دلیل ماهیت این گونه تجهیزات اغلب در محیط اینترنت کاربرد دارند و درب پشتی سخت افزاری تعبیه شده موجب می شود تا اطلاعات ذخیره شده بر روی هارد، برای هکرها در دسترس باشد.

این درب پشتی سخت افزاری و سایر آسیب پذیری ها امکان اجرای دستورات دلخواه به مهاجم و دانلود/آپلود هر فایلی را از/به سیستم ذخیره ساز می دهد. شرکت سازنده وجود این آسیب پذیری ها را تایید کرده و یک مهلت ۹۰ روزه را برای رفع آن خواستار شده است.

۲) آسیب پذیری ها

درادامه گزارشی از آسیب پذیری های شناسایی شده در هاردهای My Cloud شرکت Western Digital تشریح می گردد:

۲-۱) آپلود فایل نامحدود(بحرانی)

این آسیب پذیری که در درجه بحرانی قرار گرفته است، به مهاجم راه دور امکان می دهد تا یک فایل آلوده را بر روی سرور متصل به اینترنت و هارد آسیب پذیر آپلود کند.

این آسیب پذیری درون اسکریپت multi_uploadify.php وجود دارد که به دلیل پیاده سازی نادرست تابع gethostbyaddr() درPHP توسط برنامه نویس رخ می دهد. آسیب پذیری مورد نظر به راحتی قابل اکسپلویت است که به هکر یک شل راه دور با دسترسی root می دهد.

برای انجام این حمله و اکسپلویت آسیب پذیری آپلود فایل نامحدود، کافیست مهاجم یک درخواست Post که حاوی فایل مخرب مورد نظر است را با استفاده از پارامتر Filedata[0] ارسال کند. محل فایل آپلود شده نیز توسط پارامتر folder مشخص می شود که دارای یک هدر Host جعلی است.

ماژول اکسپلویت این آسیب پذیری درون فریم ورک رایگان متاسپلویت نیز موجود بوده و از آدرس زیر قابل دریافت است:

http://metasploit.com/download

اکسپلویت فوق از این آسیب پذیری برای آپلود یک وب شل PHP درون دایرکتوری /var/www/ استفاده می کند. وب شل مربوطه از طریق یک درخواست URI که به درب پشتی اشاره می کند، اجرا می گردد و پیلود مربوطه به آن فعال می شود.

۲-۲) درب پشتی سخت افزاری (بحرانی)

محققین طی بررسی های صورت گرفته، یک درب پشتی کلاسیک در تجهیزات مورد اشاره را شناسایی کردند که از طریق یک حساب کاربری ادمین با نام کاربری mydlinkBRionyg و پسورد abc12345cba به صورت سخت افزاری درون باینری دستگاه قابل دسترس است و بنابراین هر فردی از طریق اینترنت یا شبکه ارتباطی می تواند با این حساب کاربری به تجهیزات ذخیره سازی متصل شود. پس از لاگین هکر به سیستم کنسول مربوطه قفل می شود تا امکان تزریق آسان دستورات مخرب فراهم گردد. علاوه بر این هکر می تواند با قرار دادن یک تگ iframe یا img درون وب سایت آلوده و تشویق کاربر برای بازدید آن، کنترل دستگاه ذخیره سازی WDMyCloud را در دست گیرد. این آسیب پذیری نیز دارای طبقه بندی بحرانی است.

این درب پشتی توسط یکی از محققین شرکت امنیتی GulfTech در تاریخ ۱۲ ژوئن ۲۰۱۷ منتشر گردید که پس از گذشت ۶ ماه به دلیل عدم ارائه وصله امنیتی یا راه حل موقت از سوی شرکت سازنده، آسیب پذیری مربوطه به صورت عمومی انتشار یافت. وجود ماژول اکسپلویت آسیب پذیری درون فریم ورک رایگان متاسپلویت نشان دهنده سهولت بهره برداری همه افراد جهت حمله به تجهیزات WDMyCloud است.

۲-۳) آسیب پذیری CSRF

به دلیل اینکه هیچ گونه لایه محافظتی جهت جلوگیری از حمله CSRF درون واسط وب دستگاه WDMyCloud وجود ندارد، از طریق هر سایت آلوده ای که لینک آن توسط هکر در اختیار قربانی قرار گیرد، میتوان از طریق مرورگر وب در بستر شبکه یا اینترنت به دستگاه WDMyCloud متصل شد و به اطلاعات آن دست یافت. لذا تنها با بازکردن یک سایت آلوده(از طریق کلیک بر روی یک لینک مخرب) توسط کاربر دستگاه و بدون هیچ گونه عملیات اضافه ای، کنترل ذخیره ساز در اختیار هکر قرار می گیرد.

۲–۴) تزریق دستور

در ۴ مارچ سال ۲۰۱۷ یکی از محققین تیم امنیتی Exploitee.rs، چندین مشکل مرتبط با تزریق دستور در تجهیزات WDMyCloud را شناسایی کرد که در ترکیب با آسیب پذیری CSRF کنترل کامل دستگاه را در سطح کاربر root در اختیار هکر قرار می دهد. عملکرد واسط وب تجهیزات WDMyCloudتوسط اسکریپت های CGI مشخص می شود که مقادیر مربوط به متدهای http (post/get/cookie) را از درخواست مربوطه دریافت کرده و در فراخوانی های PHP برای اجرای دستورات شل، از آن استفاده می کند.

در بیشتر حالات، این دستورات، داده های کاربر را بدون هیچ گونه پاک‌سازی یا با پاک‌سازی بسیار محدودی مورد استفاده قرار می دهند. به عنوان مثال کد PHP زیر را در تجهیز WDMyCloud در نظر بگیرید:

```
$username = $_COOKIE['username'];
exec("wto -n \"$username\" -g", $ret);
```

کد فوق مقداری را از متغیر سراسری COOKIE انتساب می دهد که حاوی آرایه ایندکس ها برای کوکی های ارسال شده از درخواست به متغیر محلی $username است. این مقدار بلافاصله در فراخوانی تابع exec() به عنوان آرگومانی برای باینری محلی wto مورد استفاده قرار می گیرد.

به دلیل عدم انجام هیچ گونه عملیات پاکسازی در این کد، استفاده از مقدار نام کاربری به صورت username = $(touch /tmp/1) دستور exec() موجود را به صورت wto -n "$(touch /tmp/1)" –g تبدیل کرده و سپس دستوری را که حاوی ورودی کاربر است را درون آن اجرا می کند.

این قالب که در اغلب اسکریپت های درون واسط های وب مورد استفاده قرار می گیرد، منجر به آسیب پذیری تزریق دستور می شود.

۲–۵) دور زدن احراز هویت

این محقق امنیتی بیان می کند که در بررسی روش احراز هویت کاربر به سیستم از کوکی ها یا متغیرهای نشست PHP استفاده می شود که گرچه به خودی خود ایراد محسوب نمی شود ولی شیوه استفاده تجهیزات WDMyCloud در این خصوص محل اشکال است. به دلیل اینکه کوکی مربوط به احراز هویت توسط کاربر تغذیه می شود، لذا نیازمندی های مربوط به اسکریپت آن نیز ممکن است توسط هکر تامین شود و در صورتی

که هکر درون کوکی مربوطه متغیر Username را با یک مقدار دلخواه پر کرده و متغیر isAdmin را برابر ۱ قرار دهد، می تواند احرازهویت را دور بزند.

۲-۶) منع سرویس

محققین تیم Exploitee.rs بیان داشتند که به دلیل اینکه هر کاربر احرازهویت نشده ای می تواند تنظیمات سراسری زبان را برای تجهیزات ذخیره سازی و تمامی کاربران آن انجام دهد، لذا هکر با سوء استفاده از این قابلیت می تواند به راحتی شرایط حمله منع سرویس را در واسط وب دستگاه به وجود بیاورد.

۲-۷) افشای اطلاعات

طبق اظهارات محققین، یک مهاجم می تواند بدون نیاز به انجام فرآیند احراز هویت و با ارسال یک درخواست معمولی مثلاً به صورت GET /api/2.1/rest/users? HTTP/1.1 به سمت وب سرور، لیست همه کاربران تجهیز ذخیره سازی، شامل اطلاعات جزئی کاربران را دامپ کند.

۳) مدل ها و نسخه های آسیب پذیر

سیستم عامل دستگاه ذخیره سازی My Cloud و My Cloud Mirror، نسخه 2.30.165 و قبل از آن شامل تمامی آسیب پذیری های مورد اشاره فوق هستند.

مدل های تجهیزاتی که تحت تاثیر این آسیب پذیری ها قرار دارند عبارتند از :

My Cloud Gen 2, My Cloud PR2100, My Cloud PR4100, My Cloud EX2 Ultra, My Cloud EX2, My Cloud EX4, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100 and My Cloud DL4100

منابع :

1. https://thehackernews.com/2018/01/western-digital-mycloud.html
2. https://blog.exploitee.rs/2017/hacking_wd_mycloud/