آسیب‌پذیری دوربین‌های Smartcams

دوربینی که اجازه هر کاری به هکرها می‌دهد

کارشناسان امنیتی به تازگی موفق شده‌اند، آسیب‌پذیری جدیدی را در دوربین‌های Smartcams شناسایی کنند. این آسیب‌پذیری به هکرها اجازه می‌دهد تا امتیازات ریشه را روی دستگاه قربانی به دست آورده و دستورات خود را از راه دور روی آن اجرا کنند.

Smartcams یک دوربین تحت شبکه ساخت سامسونگ بوده که قادر است به سرویس‌های مختلف این شرکت متصل شده و ویدیوها و رخدادهای زنده و آنلاین را از هر مکانی پخش کند. به طوری که کاربران از هر مکانی قادر به مشاهده ویدیوها باشند. این دوربین‌ها به ویژه در ارتباط با سرویس‌های نظارت بر کودکان و حیوانات خانگی کاربرد فراوانی دارد. مالکان این دستگاه‌ها با استفاده از این دوربین‌ها و سرویس‌های جانبی آن‌ها قادر هستند یک سازوکار قدرتمند امنیتی را به وجود آورند. این دوربین‌ها به راحتی می‌توانند پیکربندی شده و قادر هستند پیام‌ها را به صورت آنی برای مالک دستگاه ارسال کنند. اما به نظر می‌رسد دوربین‌های Smartcams یکبار دیگر با مسائل امنیتی روبرو شده‌اند. به طوری که به تازگی آسیب‌پذیری جدیدی در ارتباط با این دوربین‌ها شناسایی شده است.

مطلب پیشنهادی

تازه‌های شبکه شماره 182
اولین دوربین امنیتی دی‌لینک با پشتیبانی از HomeKit اپل

سایت exploitee.rs به تازگی اعلام کرده است یک آسیب‌پذیری جدی را در محصول این شرکت شناسایی کرده است. آسیب‌پذیری فوق به هکرها اجازه می‌دهد امتیازات ریشه را روی این دستگاه به دست آورند. آسیب‌پذیری فوق را می‌توان با استفاده از یکی از سرویس‌های وب شرکت سامسونگ مورد سوء استفاده قرار داد.

آسیب‌پذیری سرور محلی

سامسونگ برای آن‌که آسیب‌پذیری‌های دوربین‌های خود را برطرف کند، واسط وب محلی را حذف کرد و کاربران را ملزم ساخت برای برقراری ارتباط خود به سایت smartcloud متصل شوند، اما در همین حال سرورهای محلی خود را بدون هیچ‌گونه تغییری در حالت فعال نگه داشت. همین موضوع باعث شده است تا هکرها بتوانند با استفاده از آسیب‌پذیری جدید یک میان‌افزار سفارشی را برای این دوربین‌ها ارسال کرده و به این شکل به واسط وب متصل شوند. کارشناسان امنیتی در این ارتباط گفته‌اند: «آسیب‌پذیری iwatch install.php را می‌توان با ساخت فایلی با نام مشخص و ذخیره‌سازی آن درون یک فرمان tar و فراخوانی آن از طریق تابع system() در پی‌اچ‌پی مورد بهره‌برداری قرار داد.» سامسونگ هنوز هیچ‌گونه وصله‌ای برای ترمیم این آسیب‌پذیری ارسال نکرده، اما بدیهی است

در اولین فرصت میان‌افزار ویژه‌ای را برای این دوربین عرضه خواهد کرد.

/mnt/custom/iwatch/web/install.php

```
46                          switch( $mode ){
47                                  case iWatchInstaller::IWL_INSTALL_MODE_MANUAL:
48                                          $this->manualInstall($file, $data);
49                                          break;
50                                  case iWatchInstaller::IWL_INSTALL_MODE_AUTO:
51                                          $this->autoInstall( );
52                                          break;
53                                  default:
54                                          header('HTTP/1.0 405 Method not supported', true, 405);
55                                          break;
56                          }
```

/mnt/custom/iwatch/web/install.php

```
66          private function manualInstall( $file, $data )
67          {
68                  // Verify  input and process firmware request
69                  if ( $this->validateFirmware($file["file"]["tmp_name"], $file["file"]["name"], $data["checksum"])) {
70                    if ($file["file"]["error"] > 0) {
71                          header('HTTP/1.0 412 Error receiving file', true, 405);
72                    } else {
73
74                          // check for existance of file and move to tmp
75                          $sourceFile = iWatchInstaller::BASE_PATH . "/" . $file["file"]["name"];
76                          if ( move_uploaded_file($file["file"]["tmp_name"],$sourceFile) ) {
77                                  // process file and complete installation
78                                  $this->installFirmware( $sourceFile );
79                          }
80                    }
81                  }
82          }
```

اما برای اطلاع بیشتر در ارتباط با آسیب‌پذیری فوق و همچنین مشاهده کد مفهومی و نحوه ترمیم این آسیب‌پذیری بدون آن‌که نیازی به وصله‌ای که سامسونگ در این ارتباط عرضه خواهد کرد نیازی داشته باشید به آدرس **smartcam exploitee** مراجعه کنید.

تاریخ انتشار:

05 بهمن 1395

نشانی منبع: https://www.shabakeh-mag.com/security/6473