1402/12/08

(امارت – ترکیه – آذربایجان – اردن)گزارش - CVE-2024-1709
بررسی و نفوذ با استفاده از آسیب پذیری

طبقه بندی: محرمانه

OFFICE
SEPEHR

{بسم الله الرحمن الرحيم}

فهرست

مقدمه

پس از انتشار آسیب پذیری بر روی نرم افزار ConnectWise در تاریخ ۲۱فوریه و پس از تلاش های انجام شده بر روی رژیم، اینبار تلاش ها برای اخذ دسترسی از اهداف مرتبط با تجهیز مذکور در کشورهای امارات، آذربایجان، ترکیه، اردن نیز انجام شد. در این گزارش به جزئیات فرایندهای طی شده و نتایج حاصل از حملات صورت گرفته اشاره شده است.

در مجموع ۴۳۲۶ آدرس IP از کشورهای مذکور استخراج و از این تعداد ۱۴ آدرس آسیب پذیر بوده و نفوذ بر روی ۵ آدرس انجام شد. (از کشور آذربایجان هیچ هدفی کشف نشده است.)

خلاصه استخراج و نتایج

کشور	تعداد استخراج شده	نفوذ موفق
امارات	۳۸۹۳	۰
ترکیه	۲۰۵	۴
اردن	۲۲۸	۱
آذربایجان	۰	۰

ترکیه

از کشور ترکیه در مجموع ۱۰ آدرس آسیب پذیر کشف و نفوذ به ۴ آدرس با موفقیت انجام شد. لیست آدرس های آسیب پذیر به شرح زیر می باشد.

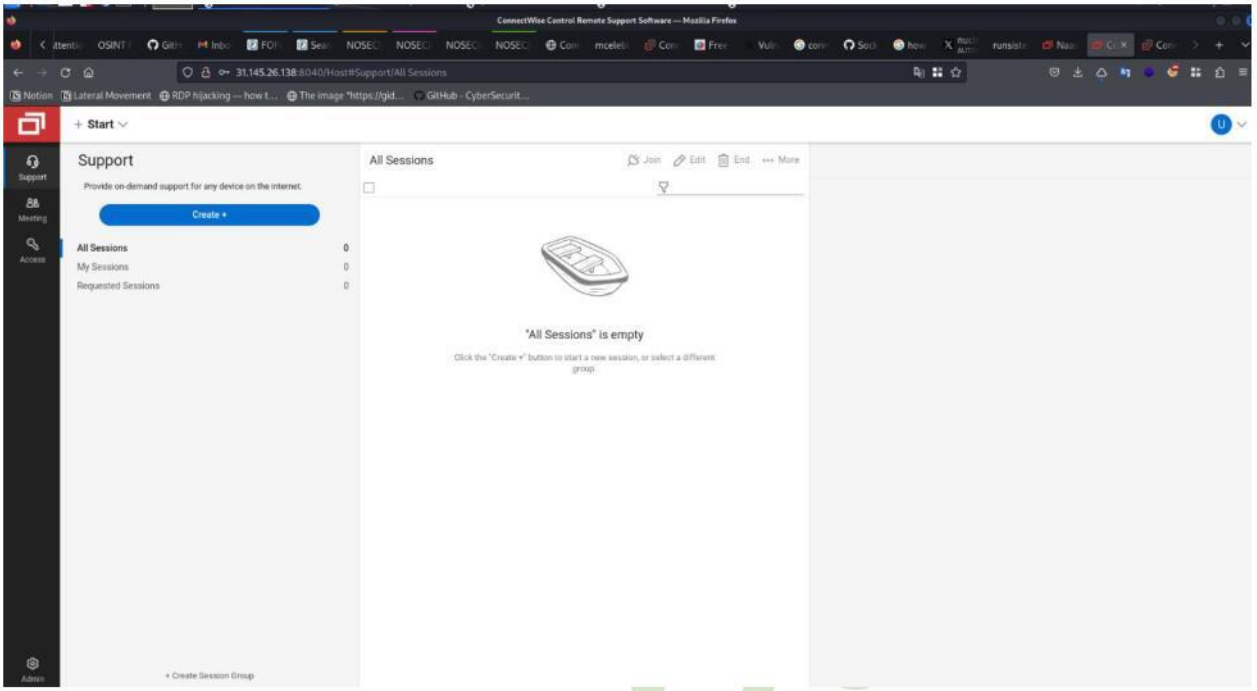
- http://77.79.124.70
- http://84.51.40.78
- http://85.105.141.253
- http://85.105.223.23:8040
- http://88.248.94.97:8040
- http://89.252.140.85:8040
- https://185.93.249.5
- http://erisim.tesannetwork.com
- https://www.puktayabaglan.com
- https://www.runsistebaglan.com

لیست آدرس هایی که نفوذ بر روی آن ها با موفقیت صورت پذیرفت به شرح زیر میباشد.

- 31.145.26.138:8040
- eclitebaglan.com
- puktayabaglan.com
- 185.93.249.51

آدرس 31.145.26.138

این آدرس بر روی درگاه ۸۰۴۰ بوده و با استفاده از آسیب پذیری مذکور بهره کشی با موفقیت صورت پذیرفت. پس از اتصال هیچ ماشین بر روی آن ثبت نشده بود.



تصویر ۱ – تصویر سامانه مدیریتی تجهیز مذکور

نام کاربری و کلمه عبور اضافه شده.

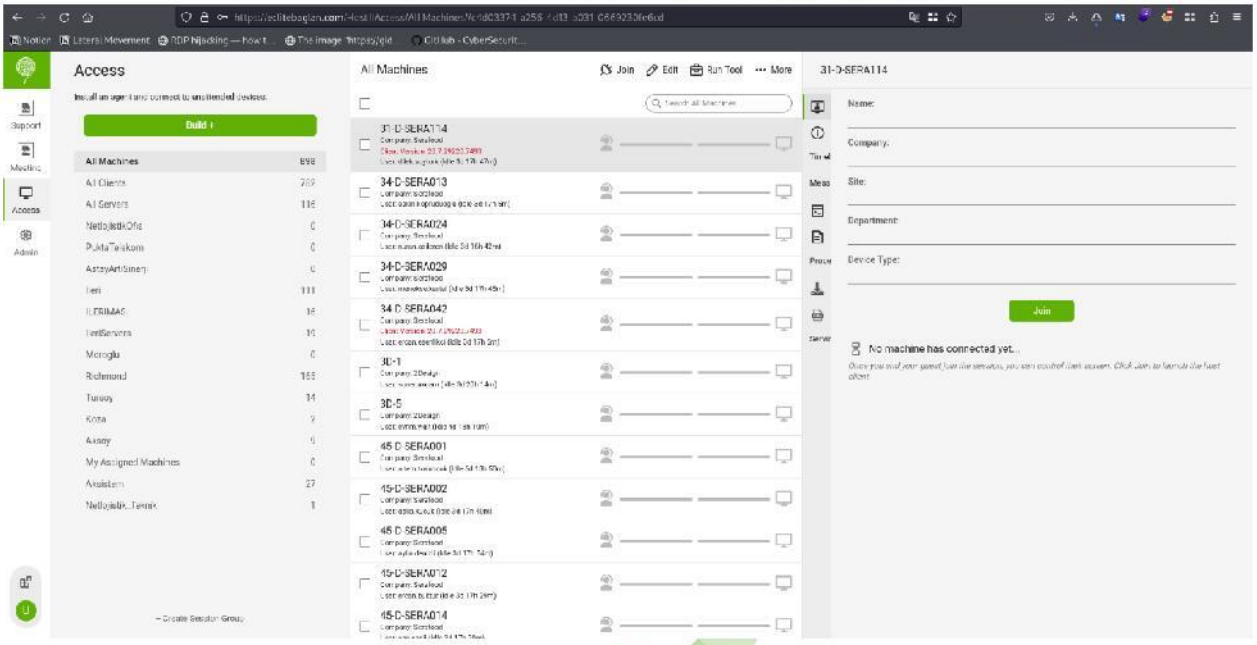
- https://31.145.26.138:8040
- Username: uuminder
- Password: U123Um10nder

نتیجه

به دلیل عدم وجود ملشین متصل، لذا اقدامی صورت نپذیرفت.

آدرس eclitebaglan.com

شرکت eclitebaglan با شعار IT Simplified متخصص در حوزه ارائه خدمات حوزه IT (فناوری اطلاعات) می باشد. در زمان نفوذ و بهره کشی از تجهیز مذکور ۸۹۸ ماشین بر روی آن فعال بودند. اما هیچ یک از این ماشین ها فعال نبودند. (احتمالا Agent ها حذف شده)



تصویر ۲ – صفحه مدیریت سامانه تجهیز مذکور

نام کاربری و کلمه عبور اضافه شده.

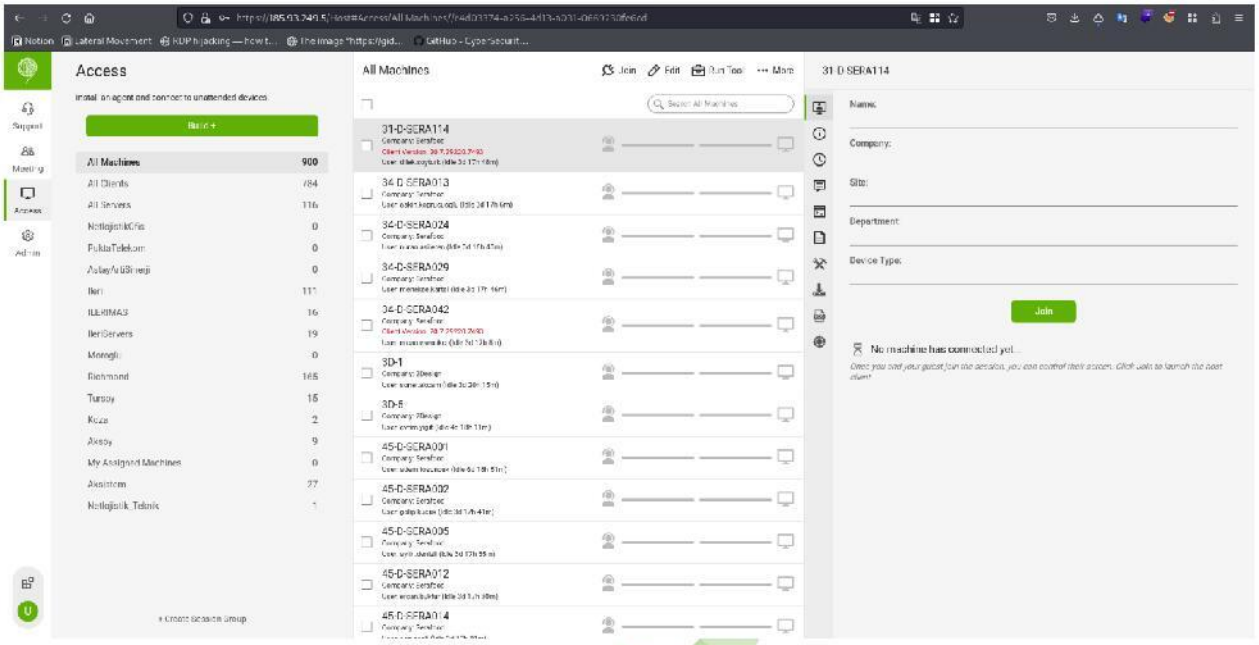
- https://eclitebaglan.com
- Username: uuminder
- Password: U123Um10nder

نتیجه

آدرس مذکور در حال حاضر (آخرین بار در تاریخ ۰۸-۱۲-۱۴۰۲) در دسترس نمی‌باشد. به دلیل غیرفعال بودن ماشین های زیرمجموعه بهره‌برداری از این تارگت میسر نبود.

آدرس 185.93.249.5

این آدرس نیز مرتبط با دامنه eclitebaglan.com بوده و در زمان تست ۹۰۰ ملشین (Session) در این تجهیز قابل مشاهده بوده و هیچ کدام فعال نبودند.



تصویر ۳- صفحه مدیریت سامانه تجهیز مذکور

نام کاربری و کلمه عبور اضافه شده.

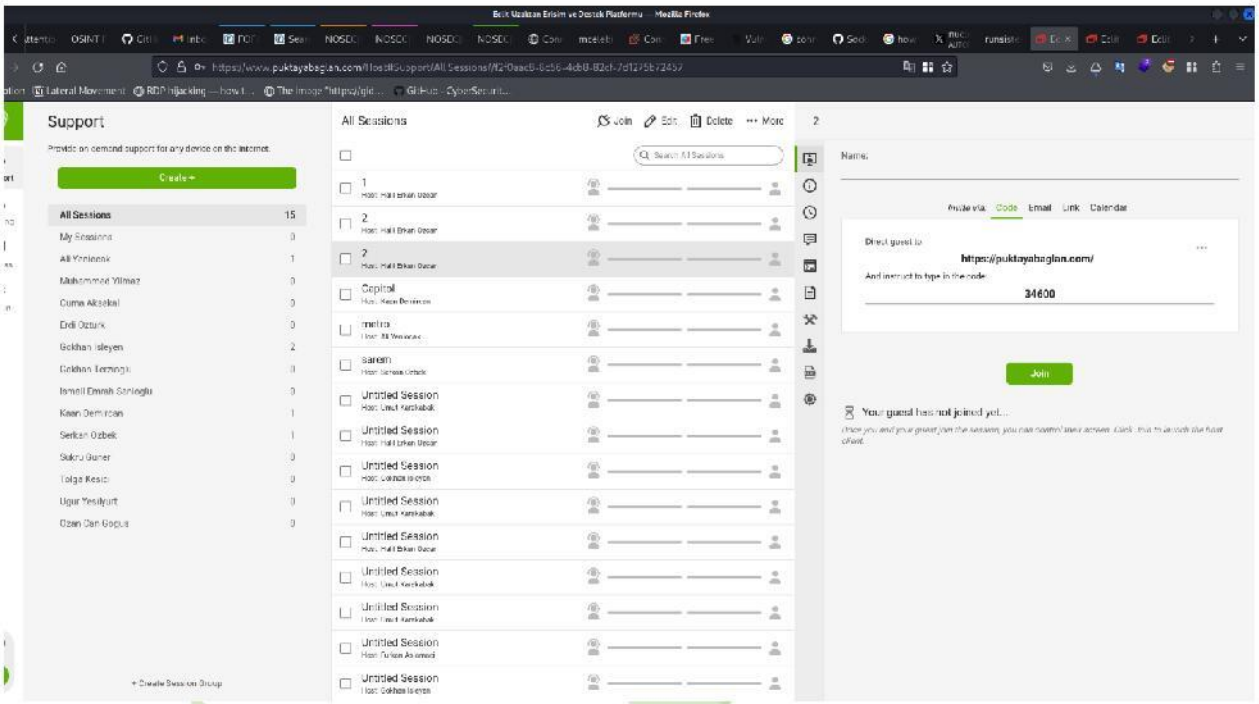
- https://185.93.249.5
- Username: uuminder
- Password: U123Um10nder

نتیجه

به دلیل غیرفعال بودن ماشین های زیرمجموعه بهره‌برداری از این تارگت میسر نبود.

آدرس puktayabaglan.com

در زمان تست و نفوذ ۱۵ ماشین بر روی تجهیز مذکور وجود داشت که از این تعداد هیچ کدام فعال نبودند.



تصویر ۴- صفحه مدیریت سامانه مذکور

نام کاربری و کلمه عبور اضافه شده.

- https://www.puktayabaglan.com
- Username: uuminder
- Password: U123Um10nder

نتیجه

به دلیل غیرفعال بودن تمامی ماشین های زیرمجموعه، بهره برداری از این تارگت میسر نمی باشد.

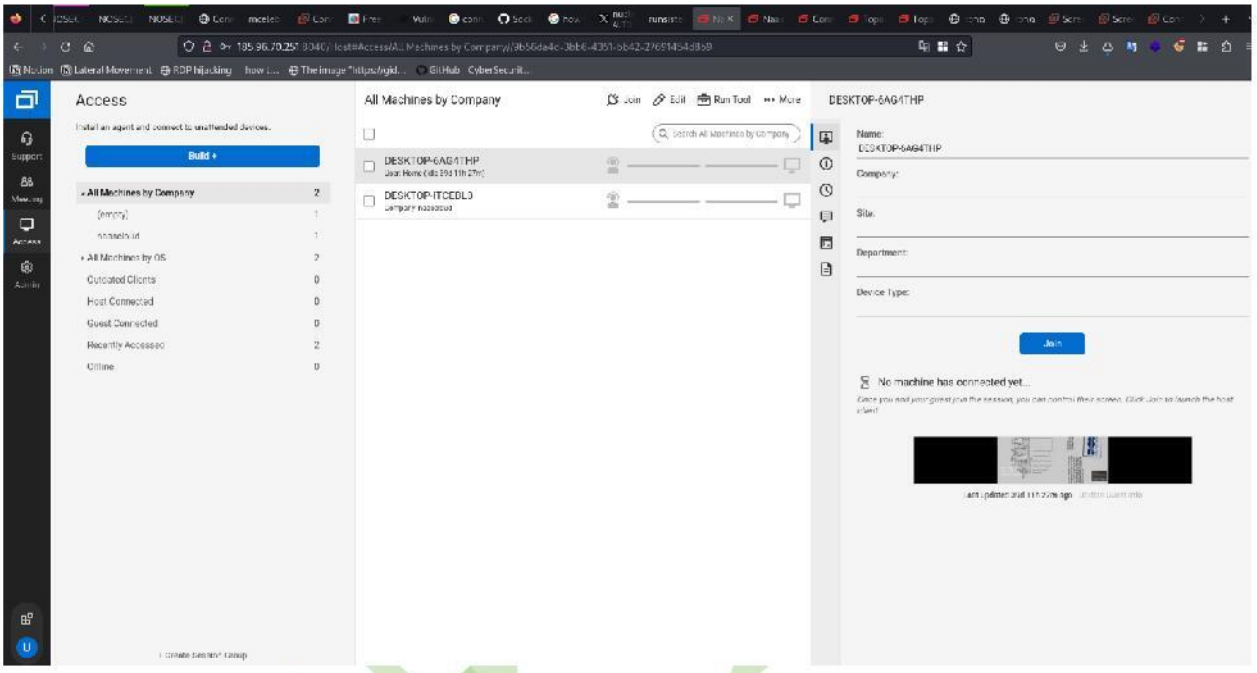
اردن

از کشور اردن مجموع ۲۲۸ آدرس IP مرتبط کشف شد، که از این تعداد ۱ آدرس آسیب پذیر و نفوذ بر روی همان آدرس با موفقیت انجام شد.

- http://185.96.70.251:8040/SetupWizard.aspx/tyafOGcytN ["ScreenConnect/22.4.7745.8154-2242049809 Microsoft-HTTPAPI/2.0"]

آدرس 185.96.70.251

در زمان تست و نفوذ تعداد ۲ ماشین زیرمجموعه در تجهیز مذکور وجود داشت که از این تعداد هیچ کدام فعال نبودند.



تصویر ۵ – صفحه سامانه مدیریتی تجهیز مذکور

نام کاربری و کلمه عبور لضافه شده.

- http://185.96.70.251:8040
- Username: uuminder
- Password: U123Um10nder

نتیجه

به علت غیرفعال بودن تمامی سیستم ها در زمان اتصال بهره برداری ممکن نبود.