> Coraz więcej urządzeń przemysłowych podłączonych do Internetu #BezpiecznyPrzemysł _

04 grudnia 2020 | Marcin Dudek (../../../../author/marcin-dudek/) | #BezpiecznyPrzemysł (../../../../tag/bezpiecznyprzemysl/), #ICS (../../../../tag/ics/), #OT (../../../../tag/ot/), #scada (../../../../tag/scada/)

CERT Polska obserwuje zwiększoną liczbę urządzeń mających związek z przemysłowymi systemami sterowania (ICS) dostępnych bezpośrednio z Internetu, często z możliwością zdalnego sterowania. Dodatkowo, jak informuje (https://us-cert.cisa.gov/ncas/alerts/aa20-205a) amerykańska agencja CISA (Cybersecurity and Infrastructure Security Agency), która obserwuje podobny trend, znane są przypadki aktorów poszukujących tego typu urządzenia i wykorzystujących ich dostępność jako wektor ataku na sieci przemysłowe.

W związku z obserwowanym zagrożeniem CERT Polska od roku prowadzi akcję #BezpiecznyPrzemysł w ramach której poszukiwane są w Internecie źle zabezpieczone urządzenia, na które atak mógłby mieć wpływ na polski przemysł. W przypadku wykrycia takiego zdarzenia, tam gdzie to możliwe, powiadamiany jest niezwłocznie właściciel wraz z rekomendacjami co do niezbędnych działań.

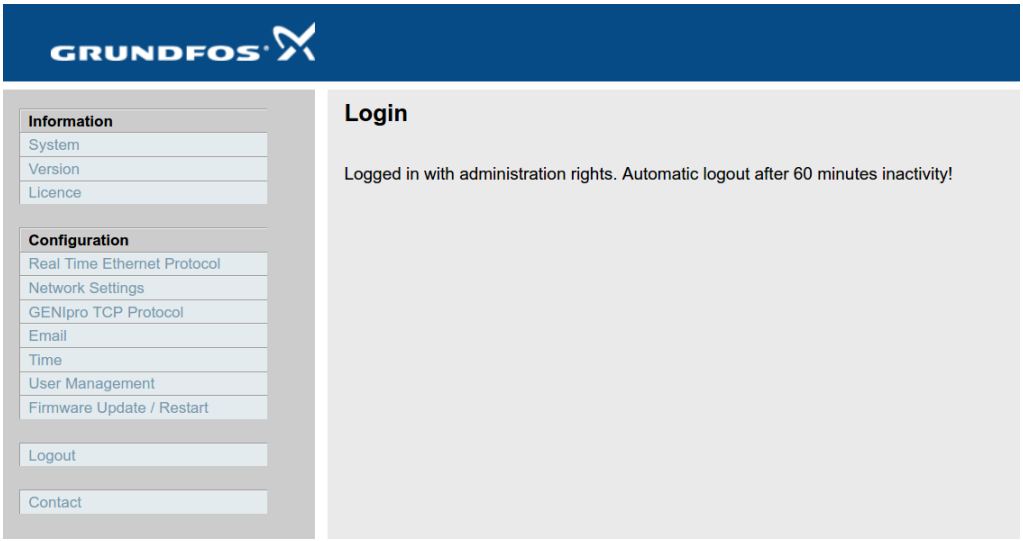
W szczególności dotyczy to urządzeń takich jak:

- Przemysłowe urządzenia sieciowe
- Moduły komunikacyjne
- Panele operatorskie
- Sterowniki PLC

W celu zobrazowania problematyki przedstawione zostaną dwie podatności odkryte przez zespół CERT Polska, które w przeszłości mogły być wykorzystane do zdalnych ataków.

Case Study #1 – Grundfos CIM 500

W grudniu 2019 odkryliśmy podatność w urządzeniach Grundfos CIM 500. Grundfos jest największym producentem pomp na świecie, z produkcją ponad 16 milionów jednostek rocznie. Moduł CIM 500 jest elementem zapewniającym tym pompom łączność sieciową. Moduł ten posiada wbudowany webserver umożliwiający konfigurację urządzenia. W momencie znalezienia podatności w Polsce było kilkanaście urządzeń tego typu widocznych bezpośrednio z Internetu, w tym urządzenia widoczne jako powiązane z oczyszczalniami ścieków.

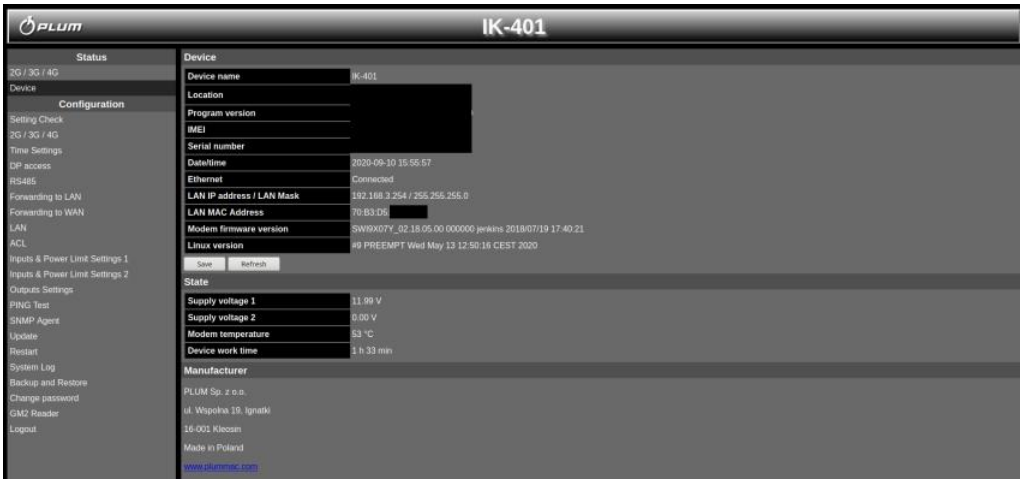


Znaleziona przez nas podatność pozwalała na pobranie konfiguracji urządzenia bez uwierzytelniania, łącznie z hasłem administratora zapisanym jawnym tekstem. Po zalogowaniu możliwa była m.in. zmiana ustawień sieciowych czy podmiana firmware'u. Podatności zostały nadane numery CVE-2020-10605 oraz CVE-2020-10609 (https://us-cert.cisa.gov/ics/advisories/icsa-20-189-01). Dla użytkowników tego modułu zaleca się aktualizację oprogramowania urządzenia przynajmniej do wersji 06.16.00.

Dodatkowo, podczas badania widoczności urządzeń z Internetu okazało się, że znaczna ich część znajduje się również poza granicami Polski. Współpracowaliśmy w tym przypadku z CERT.RO oraz Amerykańską agencją CISA.

Case Study #2 – Plum IK-401

We wrześniu 2020 odkryliśmy podatność w przemysłowych modemach polskiej produkcji – Plum IK-401. Tego typu urządzenia są często wykorzystywane w Polsce w sektorze gazowniczym oraz wodno-kanalizacyjnym. W momencie znalezienia podatności kilka takich urządzeń było widoczne z Internetu, a dodatkowo umożliwiało komunikację z kolejnymi urządzeniami wewnątrz sieci przemysłowej.



W wyniku błędnej konfiguracji webservera znaleziona podatność pozwalała na pobranie bez uwierzytelnienia m.in. pliku konfiguracyjnego zawierającego hash hasła administratora. Po zalogowaniu możliwa była konfiguracja urządzenia oraz bezpośrednio z webaplikacji komunikacja z innymi urządzeniami w sieci wykorzystując protokoły przemysłowe. Poinformowaliśmy o problemie producenta, czego rezultatem było wydanie nowej wersji oprogramowania na początku października. W związku z tym zaleca się aktualizację firmware przynajmniej do wersji 1.02.

Dla podatności został zarezerwowany numer CVE-2020-28946, a oficjalna publikacja jej szczegółów nastąpi krótko po publikacji tego artykułu.

Dalsze działania

Obserwując liczne przypadki możliwości sterowania systemami przemysłowymi przez Internet, rozesłaliśmy szczegółowe rekomendacje dotyczące tego problemu do podmiotów z sektora przemysłowego. Ogólne rekomendacje co do podnoszenia bezpieczeństwa tego typu systemów zostały również opublikowane przez CISA (https://us-cert.cisa.gov/ncas/alerts/aa20-205a) czy ACSC (https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Industrial%20Control%20Systems%20Remote%20Access%20Protocol%20%28June%202020%29.pdf).

W przypadku natrafienia na taki system dostępny z Internetu lub chęci zgłoszenia jakiejkolwiek innej nieprawidłowości mogącej mieć wpływ na cyberbezpieczeństwo instalacji przemysłowych, zachęcamy do kontaktu pod adresem cert@cert.pl lub przez stronę https://incydent.cert.pl. Dodatkowo na naszych social mediach (Facebook (https://www.facebook.com/CERT.Polska), Twitter (https://twitter.com/CERT_Polska)) w celach edukacyjnych pod tagiem #BezpiecznyPrzemysł, w przypadkach gdy jest to możliwe, dzielimy się informacjami o ciekawych znaleziskach i podatnościach.

Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne.

CERT Polska
w social mediach

Facebook (https://www.facebook.com/CERT.Polska/)

Twitter (https://twitter.com/CERT_Polska)

GitHub (https://github.com/CERT-Polska)

Kontakt

ul. Kolska 12, 01-045 Warszawa
tel.: +48 22 380 82 74
(w dni robocze, w godz. 08:30 – 16:30)
fax: +48 22 380 83 99
ePUAP: /NASK-Instytut/SkrytkaESP

e-mail: info@cert.pl (mailto:info@cert.pl)
Zgłaszanie incydentów: cert@cert.pl (mailto:cert@cert.pl)

Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”