Tiger-Team-1337

Monday, January 18, 2021

KACO XP100U HMI Credential Leak Vulnerability

Date: 2021-01-18

Author: Kevin2600

CVE: CVE-2021-3252

Version: XP-JAVA 2.0

Vendor: https://kaco-newenergy.com

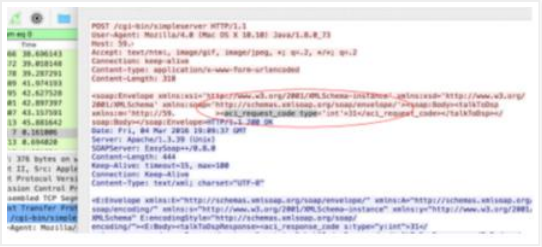
Attack Vector:

The correct credentials will be returned in plain-text from the local server, during the authentication process. Regardless of whatever the passwords have been provided.

Reproduce Steps:

1: Sniffing the authentication process of XP100U by using Wireshark or TCPDump.

2: A request "aci_request_code type='int'>31<" is sent by XP100U Client.

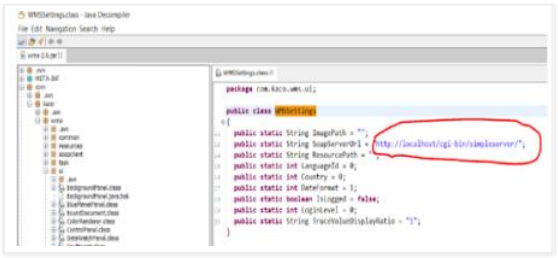


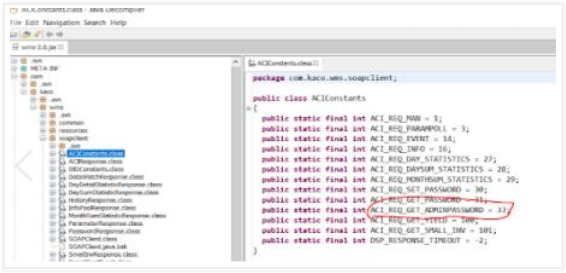
3: By reversing the java application, we can found that code 31 is used for GET_PASSWORD. And the funny part is this request actually send to the local server.

Blog Archive

May 2022 (1)
January 2022 (1)
January 2021 (1)
October 2020 (2)

Report Abuse

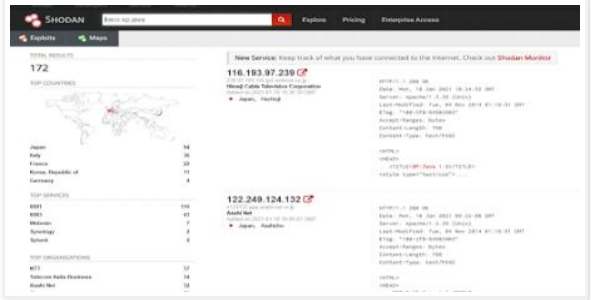




4: And regardless of whatever the passwords have been provided. The correct credentials will always be returned in PLAIN-TEXT.

Impact-Level:

From search engine Shodan. Currently, around 172 devices exposed to the public on the Internet.



Vendor Response:

The Vendor KACO has been contacted. However no response from them :(

Reference:

https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-15-224-01

at January 18, 2021

8 comments:

annisalim May 28, 2021 at 7:56 PM

365SBOBET Situs Agen Sbobet, Agen Bola Terpercaya di Indonesia

365sbobet adalah Agen SBOBET Terpercaya Indonesia, Situs Agen Bola Resmi Online Casino Terbaik Official Partner kami adalah Barcelona dan Liverpool.

agen sbobet
sbobet online
situs sbobet
situs sbobet online
situs agen sbobet
situs agen sbobet online
agen slot

slot online
situs slot
situs slot online
situs agen slot
situs agen slot online

Reply

CrownQQ Agen BandarQ June 29, 2021 at 1:33 PM

Website : CrownQQ Agen DominoQQ BandarQ dan Domino99 Online Terbesar

Yuk Buruan ikutan bermain di situs CrownQQ

Sekarang CrownQQ Memiliki Game terbaru Dan Ternama loh...

10 permainan :
* Poker Online
* Bandar Poker
* BandarQ
* Domino99
* AduQ
* Sakong
* Capsa Susun
* Bandar66 (ADU BALAK)
* Perang Baccarat
* Perang Dadu (New Games)

Bonus yang diberikan CrownQQ :
* Bonus Rollingan 0.5% Setiap Senin
* Bonus Refferal 20% Seumur Hidup
* Minimal Depo & Withdraw 20.000
* 100% Member Asli
* Pelayanan DP & WD 24 jam
* Livechat Kami 24 Jam Online

Ayo gabung sekarang juga hanya dengan
mengklick daftar crownqq

BACA JUGA BLOGSPORT KAMI:
WinCrownqq
Tips & Trik
Jendela Dunia
Berita dan Info Dunia

Info Lebih lanjut Kunjungi :
WHATSAPP : +6287771354805
LINE : CS CROWNQQ
TELEGRAM : +855882357563

Reply

nandin September 13, 2021 at 3:57 PM

MEJAQQ: AGEN JUDI POKER DOMINOQQ BANDARQ ONLINE TERBESAR DI ASIA

Yang Merupakan Agen Judi Poker DominoQQ BandarQ Online Terbesar di Asia Hadir Untuk Anda Semua Dengan Games dan Bonus Yang Menarik!

Bonus yang Kami Berikan di MEJAQQ :
* Bonus CASHBACK 0,5% 2 KALI (Dibagikan setiap hari MINGGU dan RABU)
* Bonus REFERRAL 10% + 10% SEUMUR HIDUP (Total kemenangan REFERRAL anda)
* Minimal Deposit 20,000
* Minimal Withdraw 20,000
* 7 Bank Lokal (BCA, BNI, MANDIRI, BRI, DANAMON, CIMB NIAGA, PERMATA)
* Deposit via E-Money, Pulsa TELKOMSEL dan XL (TANPA POTONGAN)
* 100% Member vs Member
* 11 Game Dalam 1 Akun
* Pelayanan Bank dan Livechat 24 jam
* Tersedia Dalam Aplikasi Android atau IOS.

Mau dapet duit tanpa kerja? Bisa banget!
Caranya? Buruan Kunjungi Sekarang Juga ^.^

Info Lebih Lanjut :
WA 1 : +85515620767
WA 2 : +855977507271

Kunjungi situs kami di :
MEJAQQ
BandarQ Online
Agen BandarQ Online

Reply

AGEN TOGEL DAN SLOT TERPERCAYA November 13, 2021 at 6:08 AM

TT4D | TOGEL TERPERCAYA | AGEN TOGEL ONLINE TERPERCAYA DI INDONESIA

TT4D Agen Togel Online TerpercayaHadiah Prize

Dengan Fiture-fiture Terbaik sebagai berikut :
• Hadiah 4D Semua Prize Semua Pasaran
• BBFS 10 Digit Tanpa Batasan Line
• Bonus Referral Sebesar 0,5% dari Semua Pemasangan Seumur Hidup
• Tersedia Slot Pragmatic , Jokerslot , Habanero , IDNPLAY

Hadiah & Diskon TT4D :
• HADIAH 4D x 3.000 (65%)
• HADIAH 3D x 400 (59%)
• HADIAH 2D x 70 (29%)

Hadiah Prize 4D (Tidak Ada 3D 2D) =
Untuk Semua Pasaran Yang Ada Prize =
Prize II : 200 Ribu (4D)
Prize III : 100 Ribu (4D
Started Prize : 55 Ribu (Hanya 4D)
Consolation : 25 Ribu (4D)
Prize di bayar pada Prize tertinggi saja dan tidak berlaku KELIPATAN.
Hadiah akan masuk ke Akun Setelah Result Pasaran.
PRIZE I NORMAL DISKON 65% HADIAH x 3000 (4D)

Website Login / Daftar :
• DAFTAR TT4D

Kontak Official :
- WA : +855963240368

• ALTERNATIF TT4D

Reply

LOADED ATM CARDS WITH VSPW W.W.W December 29, 2021 at 9:16 PM

Much obliged for tolerating me on your blog. I will carry numerous different bloggers to get your RSS roots to get more educated by your connected articles.
I tumble on a rundown of clinical affirmations courses on the web and I have chosen to impart to you the uplifting news since I realize many individuals are looking for occupations on the web, this might assist many individuals with getting utilized straightforwardly abroad.
We have examples of ATTACHED MEDICAL CERTIFICATION COURSES you can use these to get your job abroad, I will also take the advantage to ask for your permission to join our 179.3k members TELEGRAM GROUP
to share with us your ideas or any latest update on your blog.
Thanks I am Scott from Globex, we are expecting you on our platform.

Reply

hackers and programmers December 30, 2021 at 10:16 PM

I have been looking for this site for a very longtime thanks for the key information you have shared, I will help to share your blog link on my facebook page with others members on my forum.
I will also take the advantage to share with you the new UNDETECTED FAKE BANK STATEMENTS APP people are using to generate bank history for their loan approval worldwide legally , you can also join our 299.3k members TELEGRAM GROUP on how this forum operate.

Reply

Antonio Rainey January 1, 2022 at 9:10 PM

I am so delighted I found your weblog, I really found you by accident,
while I was researching on Bing for something else, Regardless I am here now and would just I saw this FAKE UK DRIVING LICENCE THAT WORKS FROM THE DVLA an will like to say thank you. (I also love the theme/design), I don't have time to go through it all at the minute but I have bookmarked it and also added your RSS feeds, so when I have time I will be back to read a lot more, Please do keep up the excellent job.

Y'all don't forget to join this DVLA EXPERTS TELEGRAM GROUP for more information about new drivers license and updated materials being used along the production process of the DL . You can also take advantage to learn and meet many Experts who will guide you on numerous techniques for anyone who love hacking and don't know how to go about it .

Reply

Aaaaccounting May 8, 2022 at 11:57 PM

The article was up to the point and described the information very effectively. Thanks to blog author for wonderful and informative post.
tax consultant in barking

Reply

To leave a comment, click the button below to sign in with Google.

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)