Kaspersky Industrial Cybersecurity Conference 2021

Vulnerability Assessment in ICS

Artem Zinenko

kaspersky

План доклада

Зачем анализировать advisory вендоров?

Примеры

Наш подход

Зачем анализировать advisory вендоров?

78%

ICS уязвимостей с «вопросами»

39%

с ошибками в условиях эксплуатации

31%

ICS уязвимостей нужно глубокое исследование

GE Multilin UR. “Factory” user

> UR devices without CyberSentry™ software option do not allow the disabling of the “Factory Mode”, which is used for servicing the IED by a “Factory” user.

GE Grid Solutions
(https://www.gegridsolutions.com/app/DownloadFile.aspx?prod=c60&type=21&file=90)

Vulnerability score: High

GE Grid Solutions
(https://www.gegridsolutions.com/app/DownloadFile.aspx?prod=c60&type=21&file=90)

CVSSv3 Base Score: 9.8

AV:N/AC:L/**PR:N**/UI:N/S:U/**C:H**/**I:H**/**A:H**

CISA (https://us-cert.cisa.gov/ics/advisories/icsa-21-075-02)


WE NEED TO GO
DEEPER

> UR devices without CyberSentry™ software option do not allow the disabling of the “Factory Mode”, which is used for servicing the IED by a “Factory” user.

GE Grid Solutions
(https://www.gegridsolutions.com/app/DownloadFile.aspx?prod=c60&type=21&file=90)

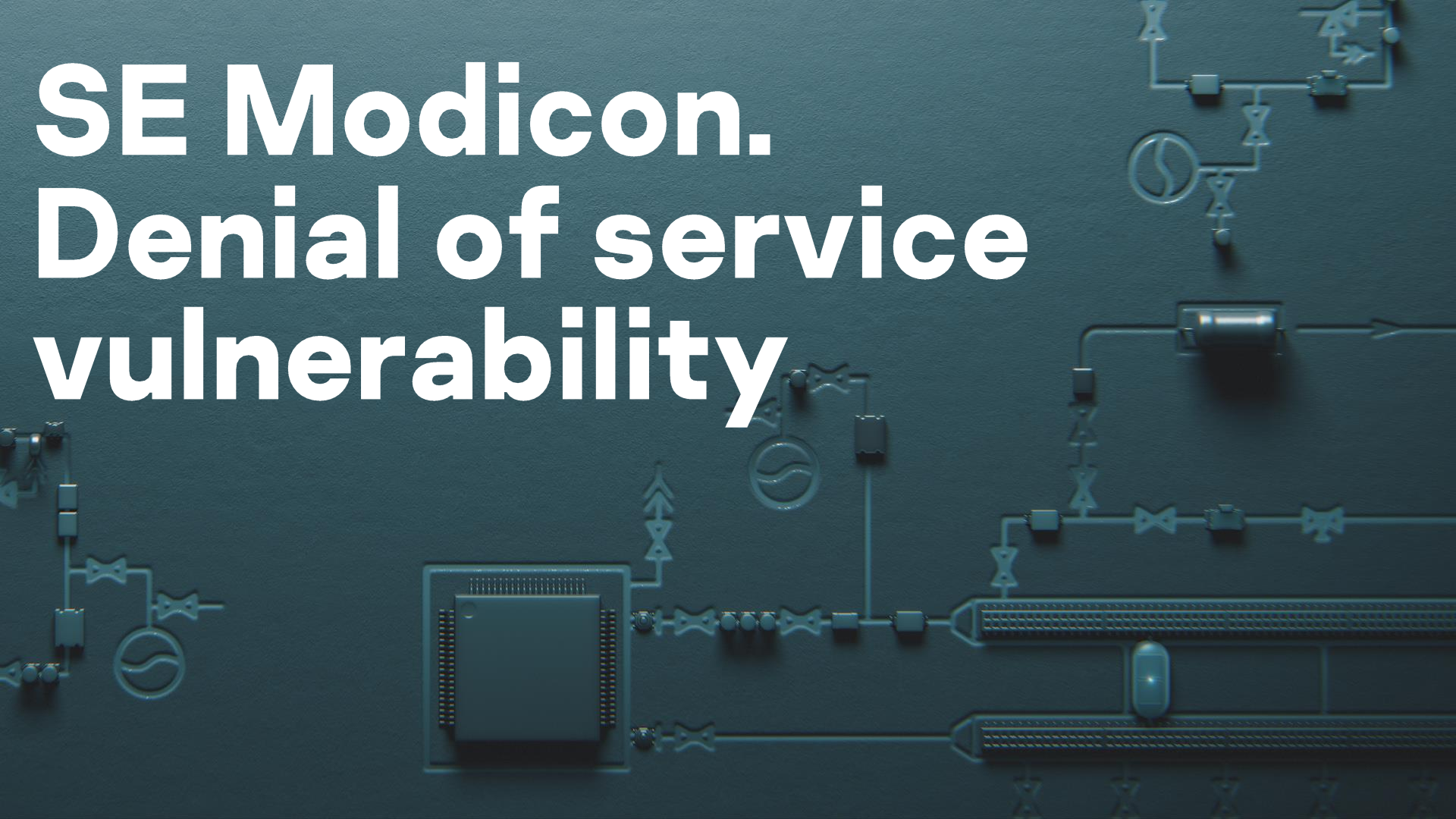

STATUS
IN SERVICE
TROUBLE
TEST MODE
TRIP
ALARM
PICKUP
VOLTAGE
CURRENT
FREQUENCY
OTHER
PHASE A
PHASE B
PHASE C
NEUTRAL / GROUND
Multilin D60 Line Distance Protection System
7
8
9
4
5
6
1
2
3
0
.
+/-
MESSAGE
ENTER
MENU
ESCAPE
RESET
HELP
VALUE
USER 1
USER 2
USER 3

Attack Vector: Network -> **Physical**
Privileges Required: None -> **High**
Confidentiality: High -> **None**

CVSSv3 Base Score: 9.8 -> **5.5**


NO VALUE

SE Modicon. Denial of service vulnerability



> A CWE-248 Uncaught Exception vulnerability exists which could cause a denial of service when sending invalid debug parameters to the controller over Modbus.

SE (https://www.se.com/ww/en/download/document/SEVD-2019-134-11/)

CVSSv3 Base Score: 7.5

AV:N/AC:L/**PR:N**/UI:N/S:U/C:N/I:N/**A:H**

SE (https://www.se.com/ww/en/download/document/SEVD-2019-134-11/)

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher(s) Name
CVE-2018-7843, CVE-2018-7844, CVE-2018-7845, CVE-2018-7850, CVE-2018-7852, CVE-2018-7853, CVE-2018-7854, CVE-2018-7855, CVE-2018-7856, CVE-2019-6806, CVE-2019-6807, CVE-2019-6808, CVE-2019-6809, CVE-2019-6828, CVE-2019-6829, CVE-2019-6830	Jared Rittle (Cisco Talos)

SE (https://www.se.com/ww/en/download/document/SEVD-2019-134-11/)

> This can be completed by first obtaining a **PLC reservation**, and then sending a data payload …

Cisco Talos (https://talosintelligence.com/vulnerability_reports/TALOS-2019-0765)


Modbus Function Code (0x5A)
Session
UMAS Function Code
Data

Резервация

Резервация

TAKE_PLC_RESERVATION
(SECRET)

Резервация

TAKE_PLC_RESERVATION
(SECRET)

SESSION

Резервация

TAKE_PLC_RESERVATION
(SECRET)

SESSION

UMAS request
with session

Резервация

TAKE_PLC_RESERVATION
(SECRET)

SESSION

UMAS request
with session

UMAS response

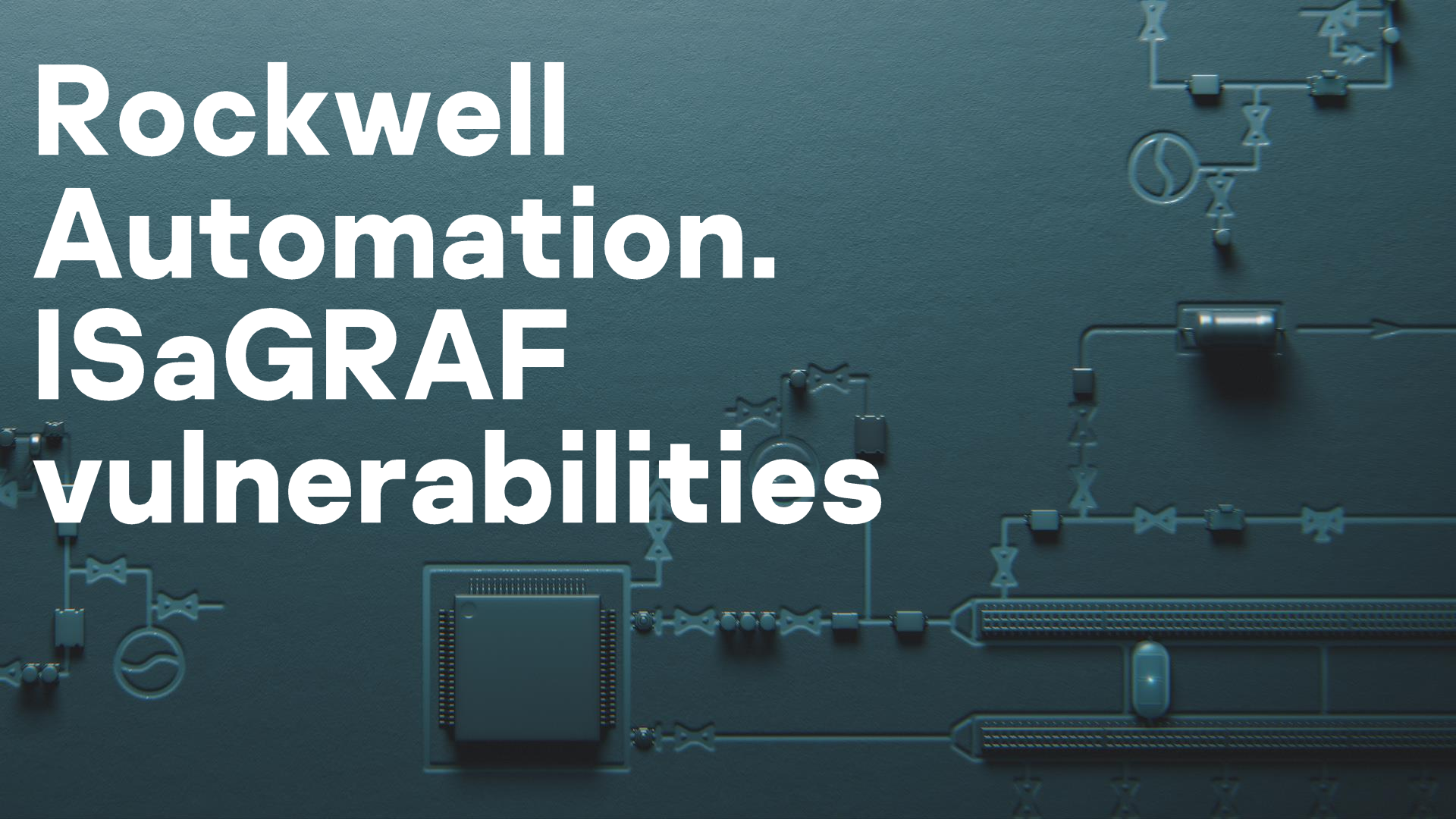
ADMIN PRIVILEGES REQUIRED!!!

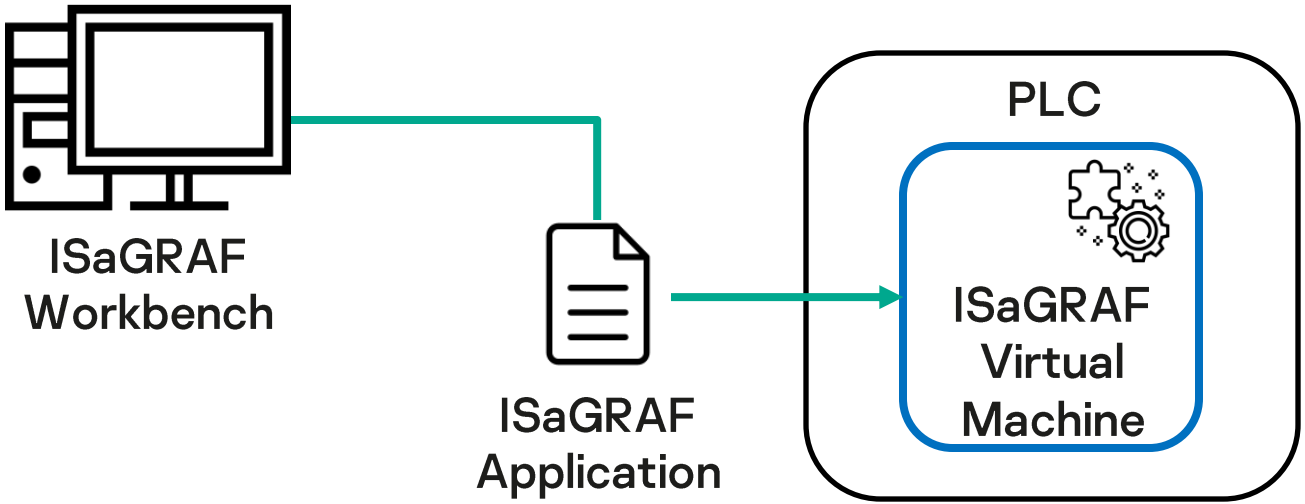
Privileges Required: None -> **High**

CVSSv3 Base Score: 7.5 -> **4.9**


NO VALUE

Rockwell Automation. ISaGRAF vulnerabilities




ISaGRAF
Workbench
ISaGRAF
Application
PLC
ISaGRAF
Virtual
Machine

8 уязвимостей, 2 RCE

~1.5 года от репорта до выпуска advisory вендором

Rockwell Automation
(https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1131699)

250

Семейств ПЛК с ISaGRAF Runtime

Кто и где использует

Leroy Automation (FR)

ISaGRAF Runtime

EKE (FIN)

ÖBB

London Underground

SNCF (FR)

Поезд Санкт – Петербург - Хельсинки

Talgo (Spain)

CAF (Spain)

Европрибор

Вымпел

Owen

Россия

SE

GE

RA

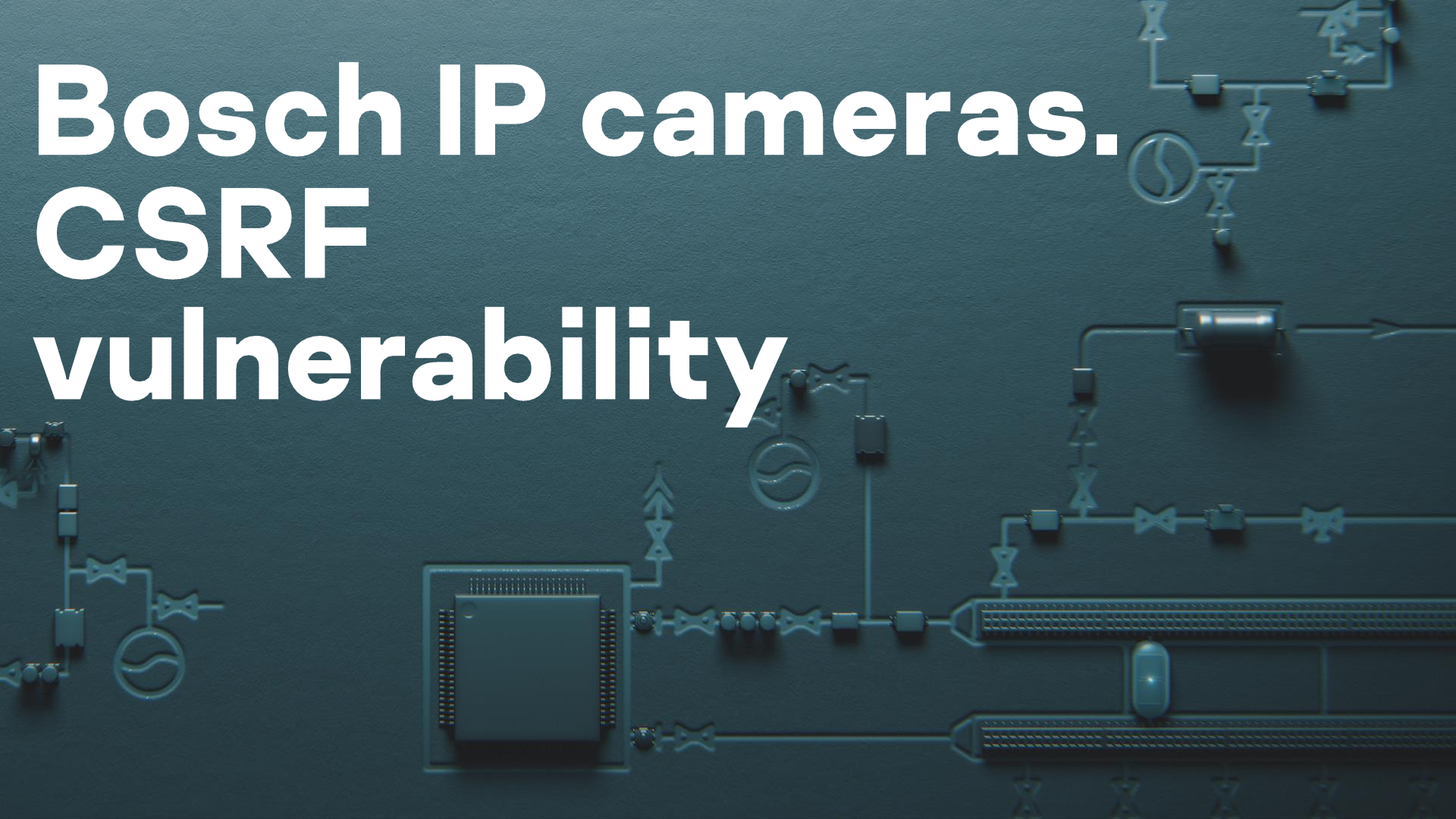
Румыния

Китай

> Программирование контроллера осуществляется с помощью среды разработки **ISaGRAF 5 Workbench**.

https://fiord.com/poisk-po-saytu/apparatnye-sredstva/programmno-apparatnye-isagraf-platformy/isagraf

Bosch IP cameras. CSRF vulnerability



> A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user.

Bosch PSIRT (https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-sa-033305-bt_cve-2021_23849_ip_cameras.pdf)

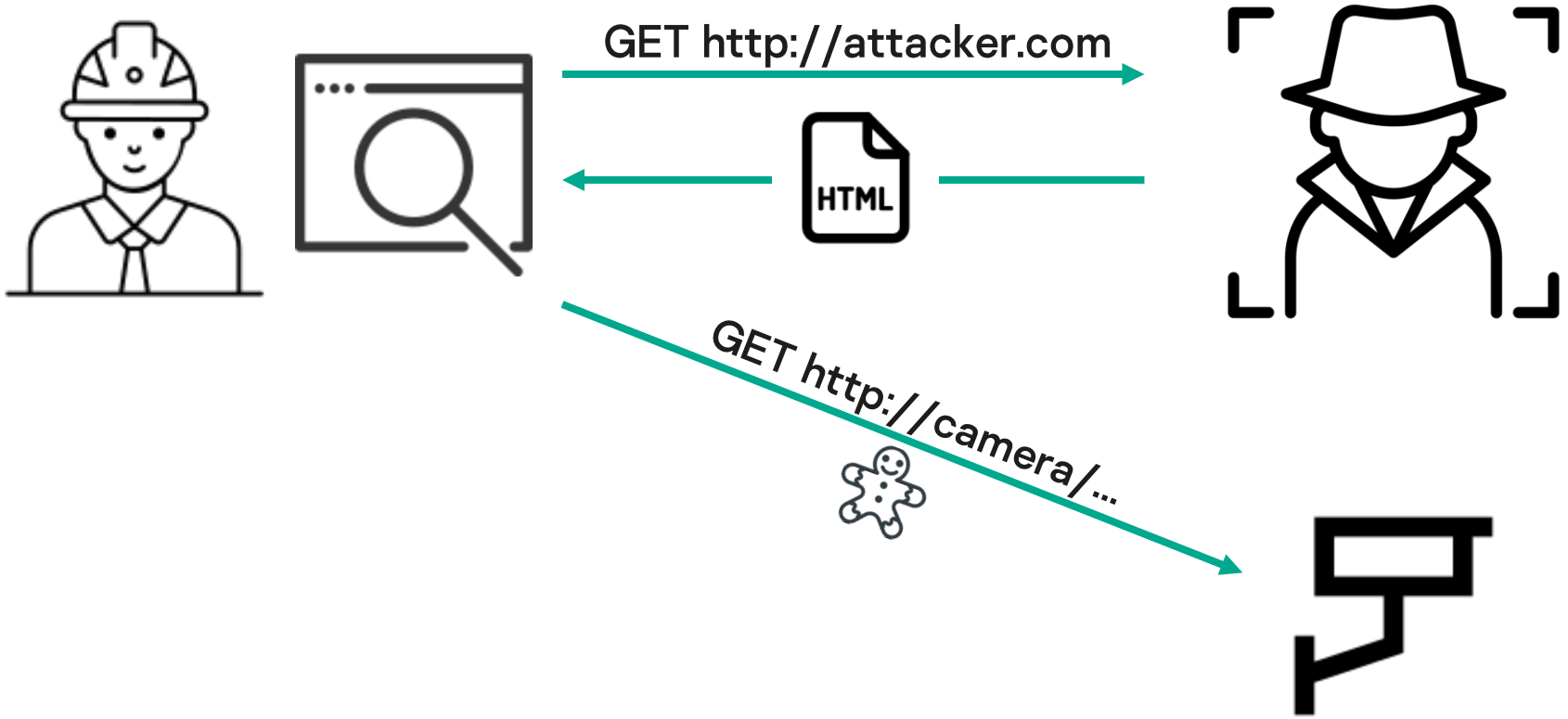
Что такое CSRF?

Что такое CSRF?

GET http://attacker.com

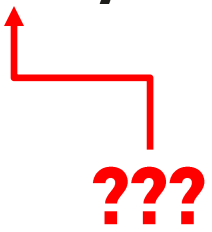
Что такое CSRF?

Что такое CSRF?

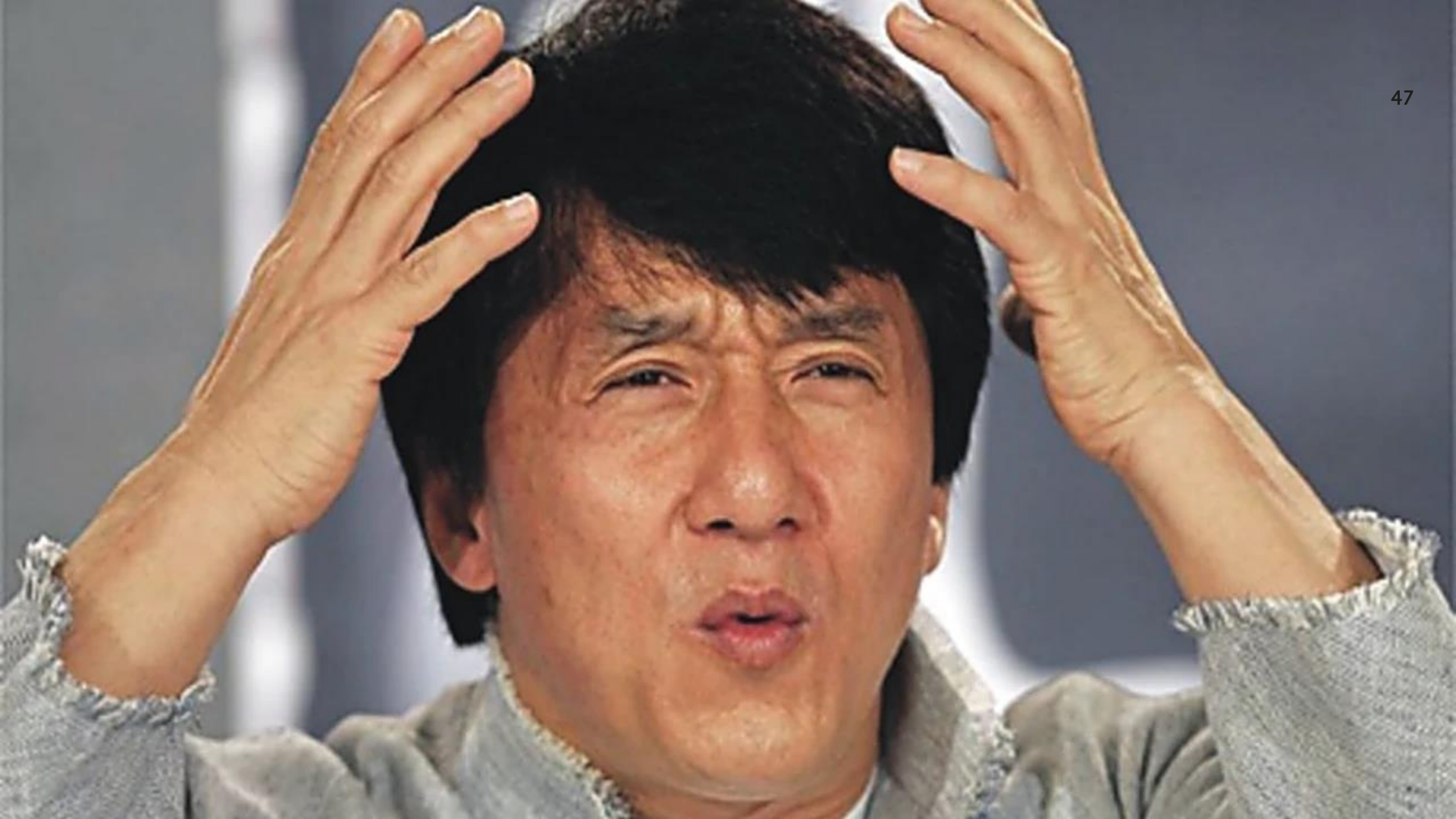


CVSSv3.1 Base Score: 7.5

AV:N/**AC:H**/PR:N/UI:R/S:U/C:H/I:H/A:H



Bosch PSIRT (https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-sa-033305-bt_cve-2021_23849_ip_cameras.pdf)

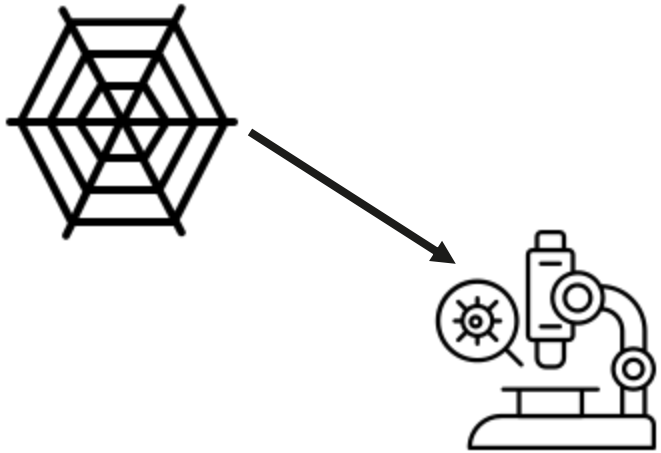


Attack Complexity: High -> **Low**

CVSSv3 Base Score: 7.5 -> **8.8**

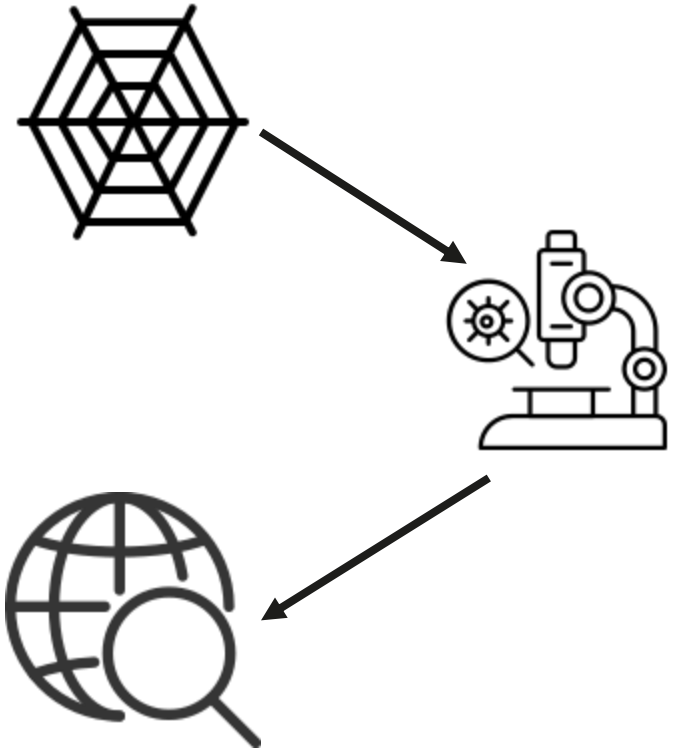
Процесс анализа уязвимостей KL ICS CERT

Мониторинг



Мониторинг

Исследование



Мониторинг

Исследование

Анализ

Чем мы можем помочь?

Kaspersky
Threat Intelligence

Kaspersky
Industrial
CyberSecurity

Kaspersky
ICS CERT Services

Thank you!

Artem.Zinenko@kaspersky.com

kaspersky