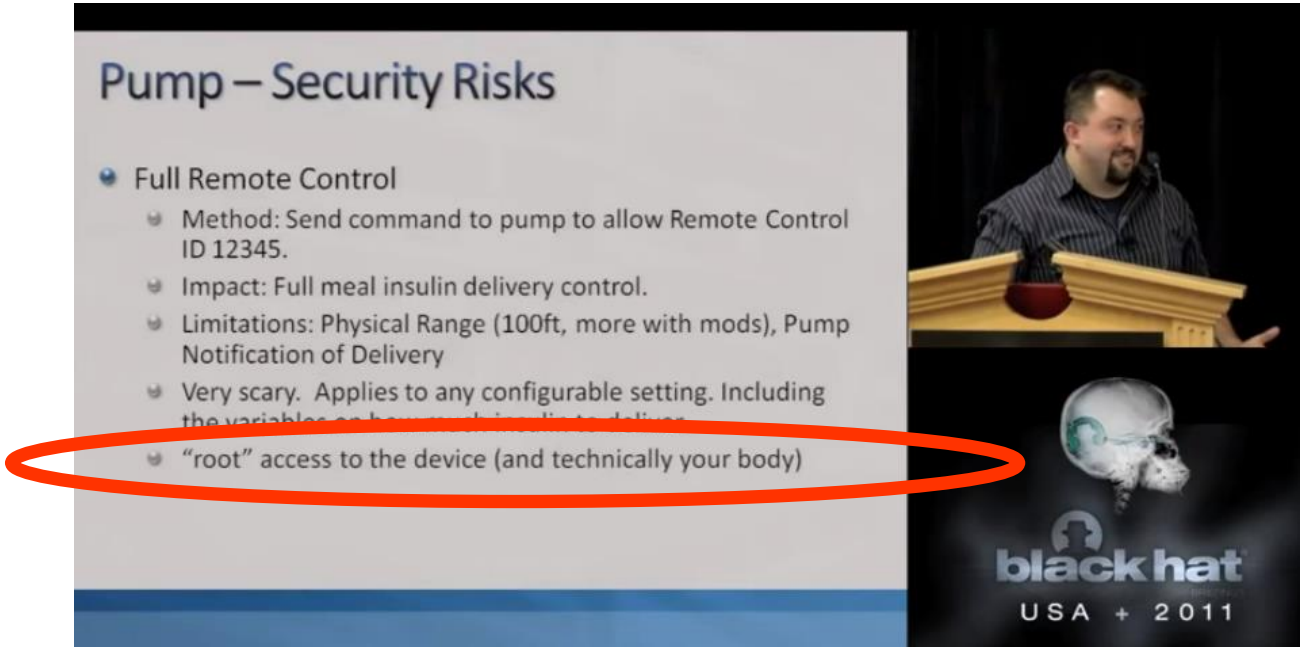
TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Healthcare e cybersecurity – Lo stato di salute della sanità digitale in Italia

Lorenzo Bracciale
Ricercatore e docente di Sanità Digitale
lorenzo.bracciale@uniroma2.it

Cosa rende la cyber-security della sanità diversa?

- *Il tipo di dati/assets da proteggere*
- *Il tipo di rischio*
- *La storia: una scelta di serie B per cybercriminali*



Talk BlackHat 2011 su un'attacco a una pompa insulinica

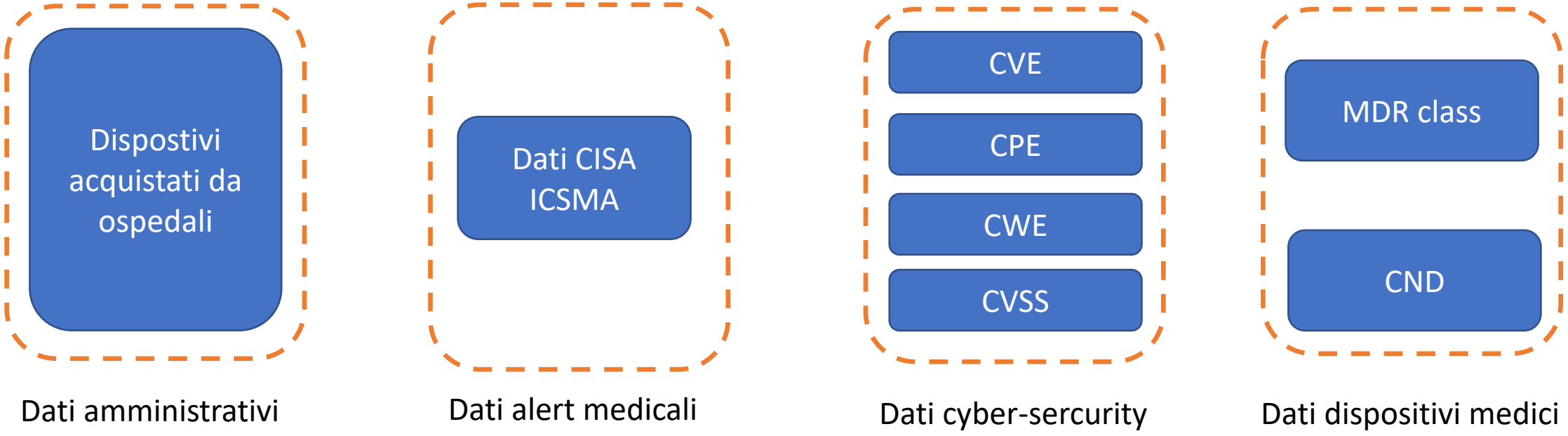
(altra) pompa insulinica portatile

Agosto 2019

- *This wireless RF communication protocol* ***does not*** *properly* ***implement authentication or authorization***
- *An* ***attacker*** *with adjacent access to one of the affected insulin pump models* ***can inject, replay, modify, and/or intercept data.***
- *This vulnerability could also allow attackers to change pump settings and* ***control insulin delivery****.*

Quale è lo stato di salute della sanità digitale in italia?

- Abbiamo costruito uno strumento di OSINT per aiutare la formulazione della stima del rischio per i dispositivi medici



Dati sugli acquisti

oggetto_gara	oggetto_principale_contratto	importo_complessivo_gara	data_pubblicazione	data_scadenza_offerta	cf_amministrazione_appaltante	denominazione_amministrazione_appaltante
LAVORI DI SOMMA URGENZA RISANAMENTO CONSERVATIVO E RIMODULAZ	LAVORI	198879.0	27/09/2018	27/09/2018	2865540799	AZIENDA SANITARIA PROVINCIALE DI CATANZARO
ACQUISTO FARMACO MODITE DEPOT DITTA BRISTOL MYERS SQUIBB SRL	FORNITURE	7210.0	25/09/2018	09/10/2018	96024110635	ASL NAPOLI 2 NORD
ACQUISTO MONITOR	FORNITURE	200.0	28/09/2018	28/09/2018	763810587	FONDAZIONE ENASARCO
ADESIONE GARA REGIONALE DPI 2^ EDIZIONE LOTTO 5 OCCHIALI AD ASTINE	FORNITURE	6534.0	20/09/2018	20/09/2018	962520110	AZIENDA UNITA SANITARIA LOCALE N. 5 SPEZZINO
AFFIDAMENTO FORNITURA PRODOTTI DI PULIZIA PER LASILO NIDO COMUN	FORNITURE	1000.0	14/09/2018	29/09/2018	627950827	COMUNE LERCARA FRIDDI
NOLEGGIO QUADRIENNALE DI VEICOLI SENZA CONDUCENTE DA ASSEGNARE	FORNITURE	34392.0	27/09/2018	27/09/2018	2253930156	COMUNE DI SESTO SAN GIOVANNI
STAGE A DUBLINO 18-19	SERVIZI	121500.0	20/09/2018	22/10/2018	97020800153	ISTITUTO TECNICO STATALE PER IL TURISMO ARTEMISIA GENTILESCHI
PROCEDURA RISTRETTA PER LA FORNITURA DI DEFLUSSORI - REGOLATORI D	FORNITURE	577400.0	07/09/2018	09/08/2021	2101050546	AZIENDA OSPEDALIERA DI PERUGIA SANTA MARIA DELLA MISERICORDIA
MANUTENZIONE HARDWARE IBM SEDE CENTRALE (GARANZIA SUL SERVIZIO	SERVIZI	112000.0	17/09/2018	02/10/2018	80054330586	CONSIGLIO NAZIONALE DELLE RICERCHE
SERVIZI DI BUSINESS INFORMATION PER LA VALUTAZIONE DELLA POSIZIONE	SERVIZI	250000.0	10/09/2018	17/09/2018	6377691008	ENEL ITALIA SPA
SERVIZ A ORDINARIA C/O LOCALI E LORO PERTINENZE	SERVIZI	81402.0	14/09/2018	24/09/2018	193460680	COMUNE DI MONTESILVANO
PI NTO TRIENNALE DI NOLEGGIO MEZZI OPERATIVI PER LA M	SERVIZI	300000.0	27/09/2018	21/11/2018	1907990012	CITTA METROPOLITANA DI TORINO
URA DI DISPOSITIVI PER STOMIE CATETERI SONDE VESCICALI E ALTR	FORNITURE	159158.68	11/09/2018	11/09/2018	1661590891	AZIENDA SANITARIA PROVINCIALE DI SIRACUSA
GGIO DI ISTRUZIONE IN ANDALUSIA	SERVIZI	72600.0	18/09/2018	01/10/2018	91081010687	LICEO SCIENTIFICO STATALE C. D'ASCANIO
AFFIDAMENTO DELLA FORNITURA DI CONTENITORI STRADALI PER LA RACC	FORNITURE	53780.0	18/09/2018	03/10/2018	1214390096	FINALE AMBIENTE S.P.A.
MANUTENZIONE PROGRAMMATA ED A GUASTO CON FORNITURA DI RICAM	SERVIZI	48229.34	03/09/2018	24/09/2018	399810589	ISTITUTO POLIGRAFICO E ZECCA DELLO STATO SPA
DAS 1676/18 - LOTTO 3 - TICOVAC TC W/NEEDLE JR 1X0.25ML SYR IT	FORNITURE	2626.0	28/09/2018	28/09/2018	1426410880	AZIENDA SANITARIA PROVINCIALE DI RAGUSA
CIG ACQUISITO PER PROROGA DEL CONTRATTO DI CUI AL CIG NUMERO 719	SERVIZI	56462.04	18/09/2018	19/09/2018	92514470159	PROVINCIA DI LODI
ACCORDO QUADRO PER LAVORI DI MANUTENZIONE OPERE DA FABBRO - SE	LAVORI	163500.0	07/09/2018	26/09/2018	2441500242	AZIENDA UNITA LOCALE SOCIO-SANITARIA N. 8 BERICA
PRODOTTI DI ROUTINE PER PATOLOGIA CLINICA R MICROBIOLOGIA IRE/ISG	FORNITURE	22256.13	03/09/2018	24/09/2018	2153140583	ISTITUTI FISIOTERAPICI OSPITALIERI
ENERGIA ELETTRICA	SERVIZI	670.32	14/09/2018	17/09/2018	5175700482	ACQUE S.P.A.
FORNITURA PIATTAFORMA TECNOLOGIA GESTIONE PROCREAZIONE MEDICA	FORNITURE	140000.0	21/09/2018	21/09/2018	6485540485	ESTAR (ENTE DI SUPPORTO TECNICO AMMINISTRATIVO REGIONALE)
ACQUISIZIONE DI SERVIZI SUPPLEMENTARI RELATIVI AL CONTRATTO DI AFFI	SERVIZI	90159.6	13/09/2018	13/09/2018	1199250158	COMUNE DI MILANO
POMPA GRUNDFOS - ORD. 67.10512	FORNITURE	736.5	06/09/2018	07/09/2018	1763190509	ACQUE SERVIZI S.R.L.
PRODUZIONE CULTURALE NELLA FATTISPECIE DELLA REALIZZAZIONE DEL LU	SERVIZI	121000.0	08/09/2018	08/09/2018	93055550771	FONDAZIONE DI PARTECIPAZIONE MATERA - BASILICATA 2019

	Struttura	Acquisto	Dispositivo
1.	UNITA SANITARIA LOCALE ROMA	MANUTENZIONE ED ASSISTENZA TECNICA ANGIOGRAFO INNOVA 2000 01/012014-30/04/2014	innova 2000 firmware

Dati sugli acquisti

oggetto_gara	oggetto_principale_contratto	importo_complessivo_gara	data_pubblicazione	data_scadenza_offerta	cf_amministrazione_appaltante	denominazione_amministrazione_appaltante
LAVORI DI SOMMA URGENZA RISANAMENTO CONSERVATIVO E RIMODULAZ	LAVORI	198879.0	27/09/2018	27/09/2018	2865540799	AZIENDA SANITARIA PROVINCIALE DI CATANZARO
ACQUISTO FARMACO MODITE DEPOT DITTA BRISTOL MYERS SQUIBB SRL	FORNITURE	7210.0	25/09/2018	09/10/2018	96024110635	ASL NAPOLI 2 NORD
ACQUISTO MONITOR	FORNITURE	200.0	28/09/2018	28/09/2018	763810587	FONDAZIONE ENASARCO
ADESIONE GARA REGIONALE DPI 2^ EDIZIONE LOTTO 5 OCCHIALI AD ASTINE	FORNITURE	6534.0	20/09/2018	20/09/2018	962520110	AZIENDA UNITA SANITARIA LOCALE N. 5 SPEZZINO
AFFIDAMENTO FORNITURA PRODOTTI DI PULIZIA PER LASILO NIDO COMUN	FORNITURE	1000.0	14/09/2018	29/09/2018	627950827	COMUNE LERCARA FRIDDI
NOLEGGIO QUADRIENNALE DI VEICOLI SENZA CONDUCENTE DA ASSEGNARE	FORNITURE	34392.0	27/09/2018	27/09/2018	2253930156	COMUNE DI SESTO SAN GIOVANNI
STAGE A DUBLINO 18-19	SERVIZI	121500.0	20/09/2018	22/10/2018	97020800153	ISTITUTO TECNICO STATALE PER IL TURISMO ARTEMISIA GENTILESCHI
PROCEDURA RISTRETTA PER LA FORNITURA DI DEFLUSSORI - REGOLATORI D	FORNITURE	577400.0	07/09/2018	09/08/2021	2101050546	AZIENDA OSPEDALIERA DI PERUGIA SANTA MARIA DELLA MISERICORDIA
MANUTENZIONE HARDWARE IBM SEDE CENTRALE (GARANZIA SUL SERVIZI						CONSIGLIO NAZIONALE DELLE RICERCHE
SERVIZI DI BUSINESS INFORMATION PER LA VALUTAZIONE DELLA POSIZION						ENEL ITALIA S.P.A.
SERVIZ A ORDINARIA C/O LOCALI E LORO PERTINENZE						COMUNE TESILVANO
PI NTO TRIENNALE DI NOLEGGIO MEZZI OPERATIVI PER LA I						CITTA ME A DI TORINO
URA DI DISPOSITIVI PER STOMIE CATETERI SONDE VESCICALI E ALTR						AZIENDA SA NCIALE DI SIRACUSA
GGIO DI ISTRUZIONE IN ANDALUSIA						LICEO SCIENTIFICO STA D'ASCANIO
AFFIDAMENTO DELLA FORNITURA DI CONTENITORI STRADALI PER LA RACC						FINALE AMBIENTE S.P.A.
MANUTENZIONE PROGRAMMATA ED A GUASTO CON FORNITURA DI RICAM						ISTITUTO POLIGRAFICO E ZEC DELLO STATO SPA
DAS 1676/18 - LOTTO 3 - TICOVAC TC W/NEEDLE JR 1X0.25ML SYR IT						AZIENDA SANITARIA PROVINCI DI RAGUSA
CIG ACQUISITO PER PROROGA DEL CONTRATTO DI CUI AL CIG NUMERO 71						PROVINCIA DI LODI
ACCORDO QUADRO PER LAVORI DI MANUTENZIONE OPERE DA FABBRO - S						AZIENDA UNITA LOCALE SOCIO-SA ITARIA N. 8 BERICA
PRODOTTI DI ROUTINE PER PATOLOGIA CLINICA R MICROBIOLOGIA IRE/ISG						ISTITUTI FISIOTERAPICI OSPITALIERI
ENERGIA ELETTRICA						ACQUE S.P.A.
FORNITURA PIATTAFORMA TECNOLOGIA GESTIONE PROCREAZIONE MEDIC						ESTAR (ENTE DI SUPPORTO TECNICO AMMINISTRATIVO REGIONALE)
ACQUISIZIONE DI SERVIZI SUPPLEMENTARI RELATIVI AL CONTRATTO DI AFF						COMUNE DI MILANO
POMPA GRUNDFOS - ORD. 67.10512						ACQUE SERVIZI S.R.L.
PRODUZIONE CULTURALE NELLA FATTISPECIE DELLA REALIZZAZIONE DEL LU						FONDAZIONE DI PARTECIPAZIONE M TERA - BASILICATA 2019

1. EXECUTIVE SUMMARY

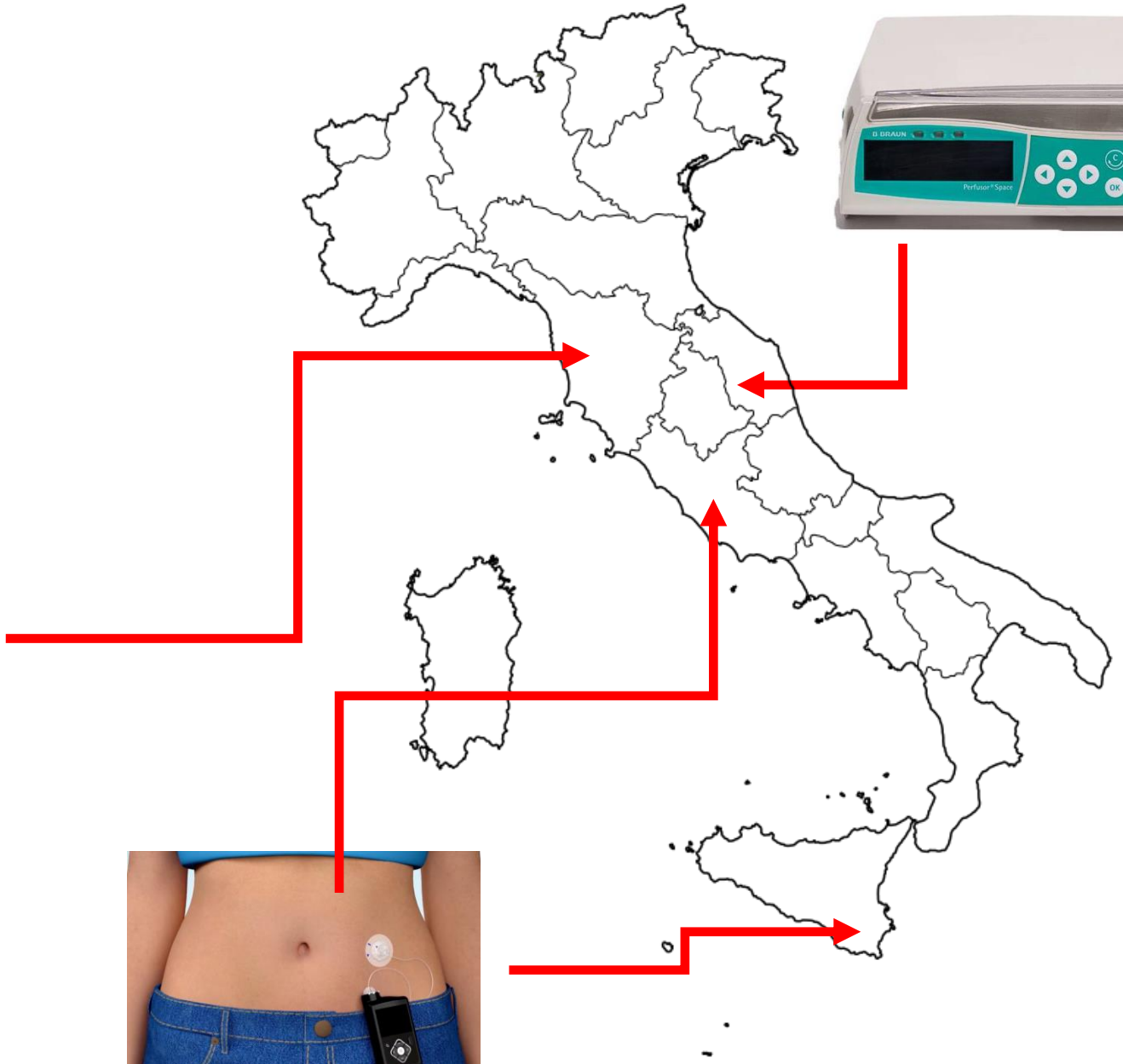
- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** GE Healthcare
- **Equipment:** GE Imaging and Ultrasound Products
- **Vulnerabilities:** Unprotected Transport of Credentials, Exposure of Sensitive System Information to an Unauthorized Control Sphere

	Struttura	Acquisto	Dispositivo
1.	UNITA SANITARIA LOCALE ROMA	MANUTENZIONE ED ASSISTENZA TECNICA ANGIOGRAFO INNOVA 2000 01/012014-30/04/2014	innova 2000 firmware

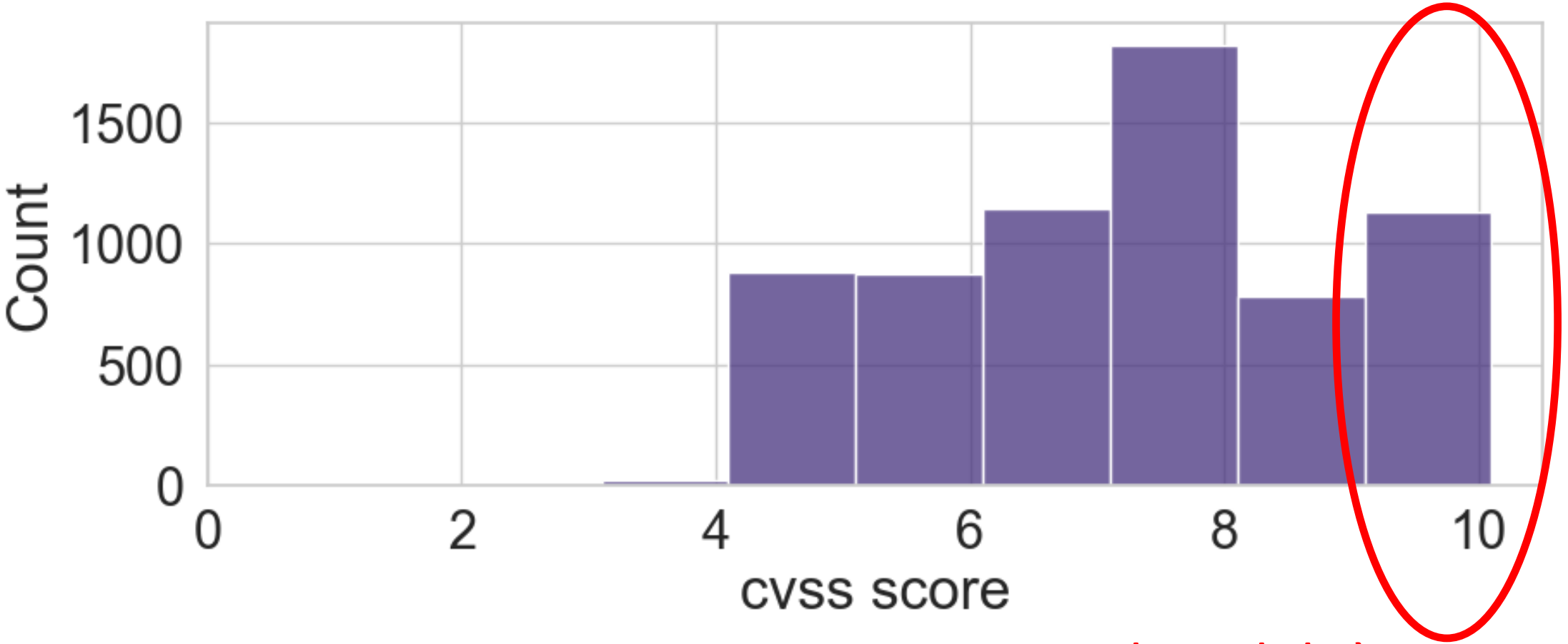
L'analisi

Dati analizzati	56M
Dati	2011-2022
Strutture sanitarie italiane	400
Acquisti relativi a dispositivi con vulnerabilità note	7000
Dispositivi medici unici con vulnerabilità note	166

Risultato



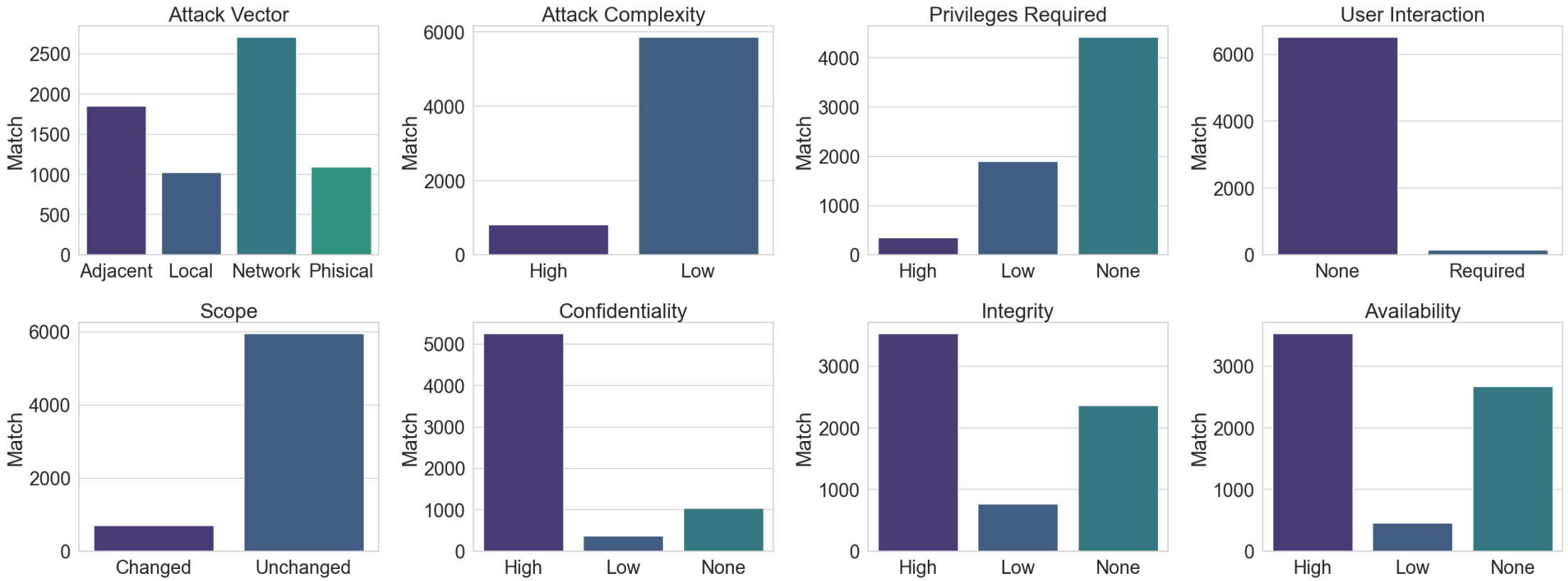
Gravità delle vulnerabilità



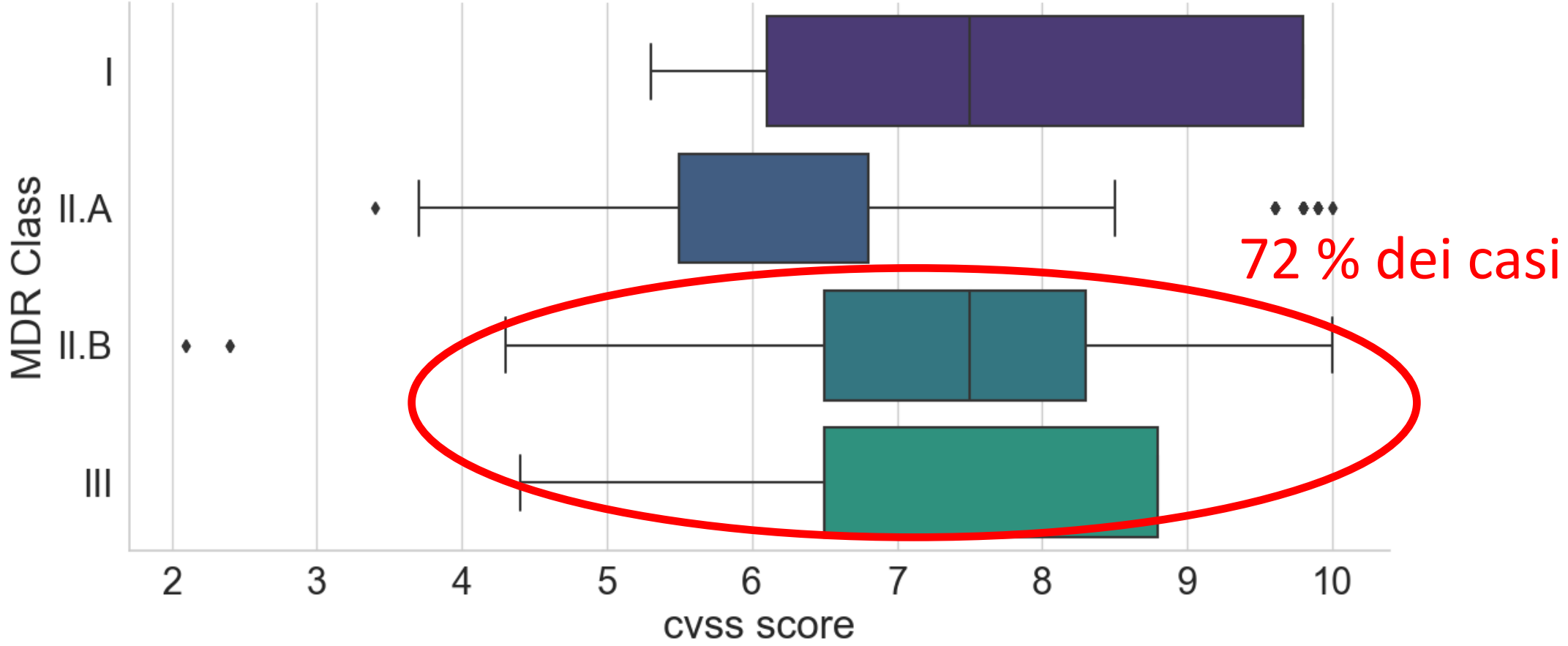
20 % vulnerabilità CRITICHE

(il doppio rispetto alla media CVE)

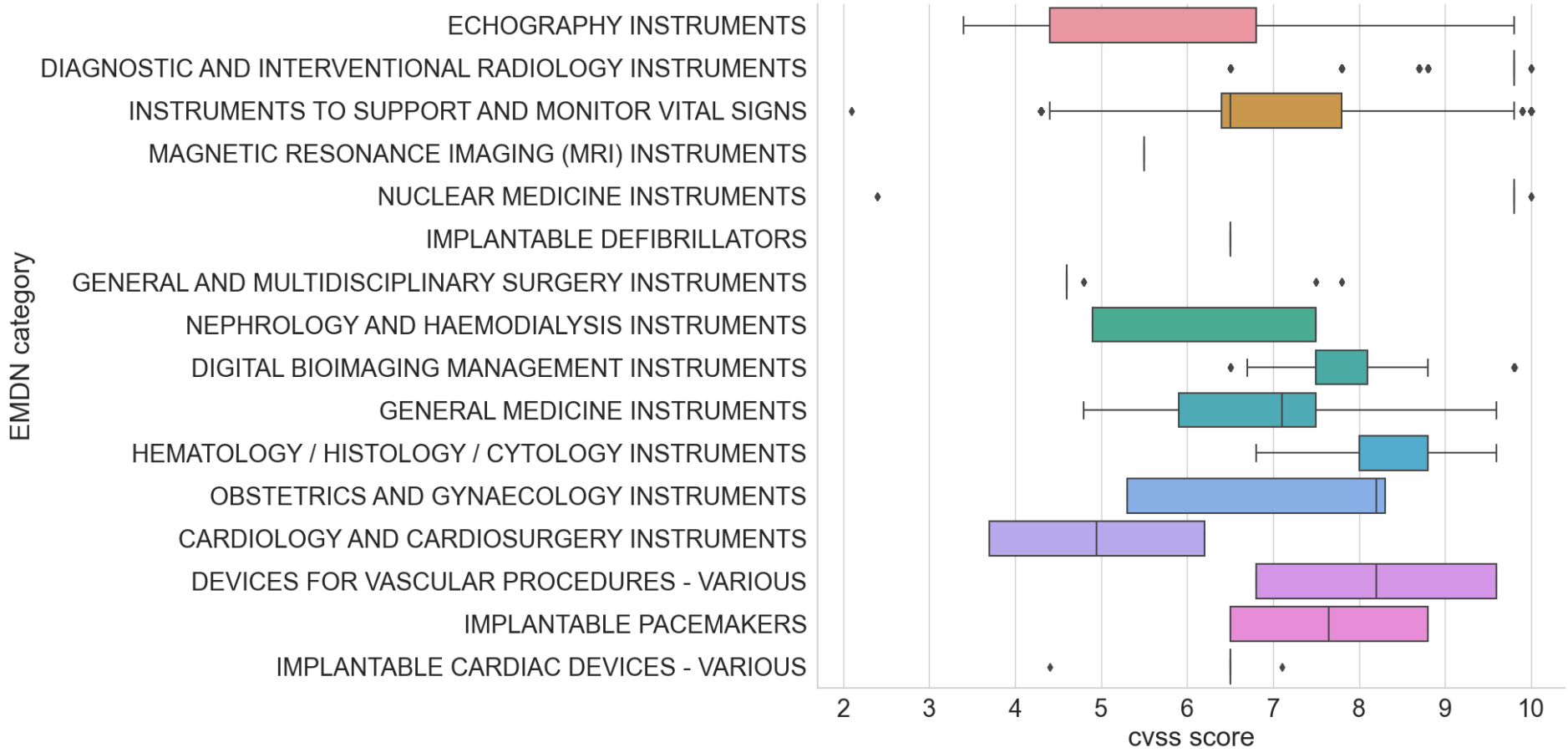
Perché queste vulnerabilità sono critiche?



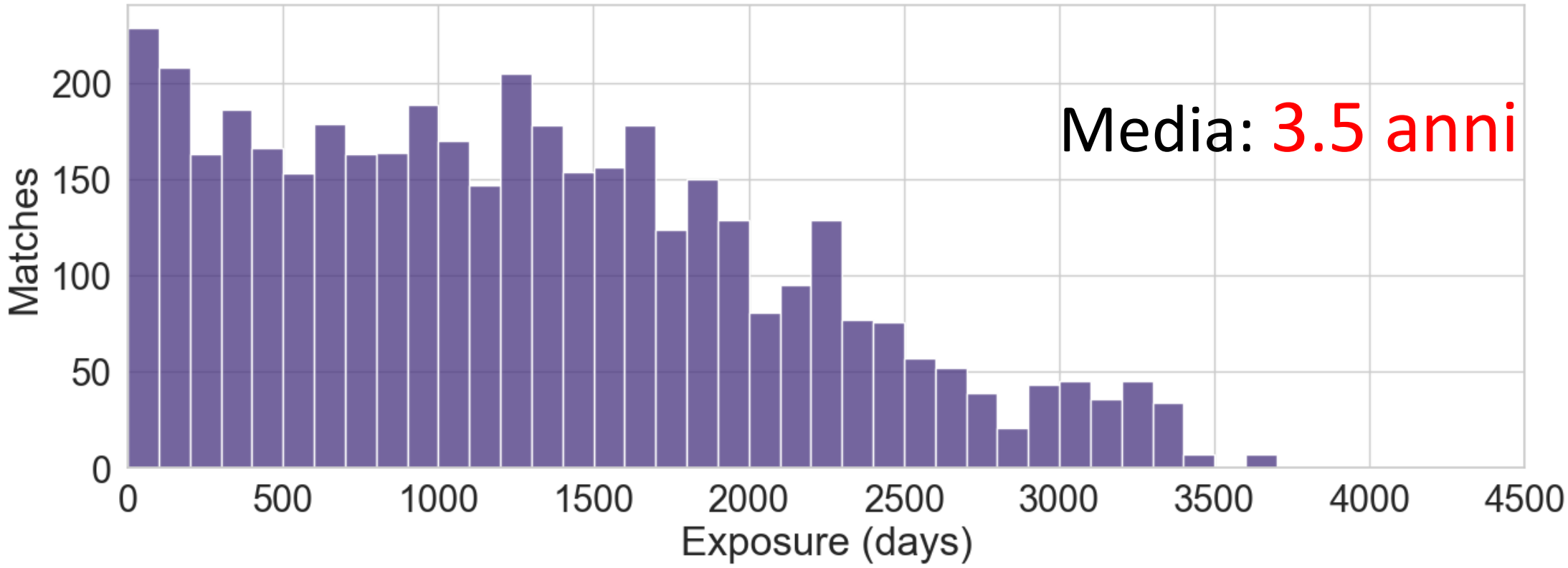
Classi di rischio (MDR)



Tipologie di dispositivi interessati (CND)



Esposizione dei sistemi



Debolezze

cwe	occurrences	ratio
CWE-200	2305	0.090784
CWE-798	2257	0.088893
NVD-CWE-noinfo	2142	0.084364
CWE-522	1965	0.077393
CWE-20	1818	0.071603
CWE-287	1643	0.064711
CWE-319	1452	0.057188
NVD-CWE-Other	873	0.034384
CWE-523	828	0.032611
CWE-434	811	0.031942
CWE-269	807	0.031784
CWE-259	794	0.031272

Information exposure

Hard coded credentials

Insufficiently protected credentials

Improper input validation

Improper authentication

…

Why? Security vs Safety

- "*McAfee Enterprise ATR Uncovers Vulnerabilities in Globally Used B. Braun Infusion Pump*" -- Douglas McKee and Philippe Laulheret - 2021
  - CVE-2021-33886 – Use of Externally-Controlled Format String (CVSS 7.7)
  - CVE-2021-33885 – Insufficient Verification of Data Authenticity (CVSS 9.7)
  - CVE-2021-33882 – Missing Authentication for Critical Function (CVSS 8.2)
  - CVE-2021-33883 – Cleartext Transmission of Sensitive Information (CVSS 7.1)
  - CVE-2021-33884 – Unrestricted Upload of File with Dangerous Type (CVSS 5.8)
- Designed for safety:
  - "*the main processing but also has a control processor that makes sure nothing unexpected occurs*"
  - "*Everything is CRC checked multiple times to flag memory corruption and every range is bounds-checked*"
- ...Not for security:
  - Everything is trusted! (Lack of authentication for custom protocols)

Quale futuro?

- Un problema difficile da gestire a causa di:
  - Cicli di vita dei dispositivi molto lunghi
  - Iter di certificazione lunghi (MDR)
  - Difficoltà in patching e recall
- La situazione sta cambiando
  - Marzo 2022 PATCH Act (Protecting and Transforming Cyber Health Care Act)
  - Gli aggiornamenti devono essere fatti dai produttori per tutta la durata della vita dei dispositivi
  - S-BOM (Software Bill Of Materials): le dipendenze software devono essere esplicite (e.g. Java, Log4j, Microsoft Windows)

MDS^2 per la valutazione della sicurezza

- MDS2 = Manufacturer Disclosure Statement for Medical Device Security
  - Sviluppato da Natl. Electrical Manufacturers Assoc. (NEMA)
- Standard volontario: i produttori di dispositivi medici possono usarlo per condividere informazioni di sicurezza
- Questionario – si focalizza su ruoli e responsabilità; migliora la trasparenza e la valutazione della sicurezza
  - 2019 version → 216 domande su 23 funzionalità di sicurezza security

Domande di esempio:

- ➔ How can the connected medical device be patched?
- ➔ Does it require physical access, or can updates be provided remotely?
- ➔ Can the operator install patches on their own, or does it all need to go through the vendor?
- ➔ Are there any built-in security safeguards and capabilities such as encryption, auto-logoff, malware detection, or physical locks?
- ➔ Does the device have anti-malware software? If not, can it be installed by the operator?
- ➔ What types of private data are stored on the device, and how are they transmitted?

Le risposte vero/falso sono solo un inizio...

MDS2 STCF-1

298		**HEALTH DATA STORAGE CONFIDENTIALITY (STCF)**	
299		*The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.*	
300	STCF-1	Can the device encrypt data at rest?	Yes
301	STCF-1.1	Is all data encrypted or otherwise protected?	
302	STCF-1.2	Is the data encryption capability configured by default?	
303	STCF-1.3	Are instructions available to the customer to configure encryption?	
304	STCF-2	Can the encryption keys be changed or configured?	
305	STCF-3	Is the data stored in a database located on the device?	
306	STCF-4	Is the data stored in a database external to the device?	

Yes
No
N/A
See Notes

E ancora:
Power/EM side channel?
Timing channels?

Servono esperti

Ma serve approfondire
Come cifri? AES ☺
Quale AES? GCM ☺
Che vettore di inizializzazione usi?

Home › Notes › VU#490028

Microsoft Windows Netlogon Remote Protocol (MS-NRPC) uses insecure AES-CFB8 initialization vector

Vulnerability Note VU#490028

Original Release Date: 2020-09-16 | Last Revised: 2021-03-19

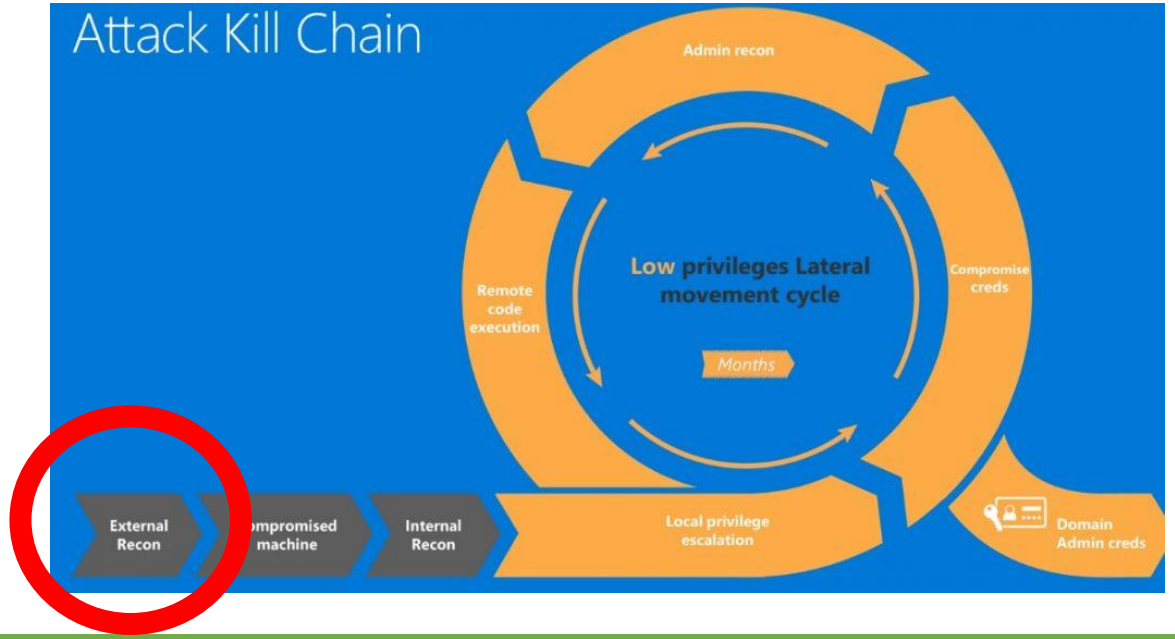
Overview

The Microsoft Windows Netlogon Remote Protocol (MS-NRPC) reuses a known, static, zero-value initialization vector (IV) in AES-CFB8 mode. This allows an unauthenticated attacker to impersonate a domain-joined computer, including a domain controller, and potentially obtain domain administrator privileges.

E se cambia il threat model?

L'italia è il secondo paese al mondo per attacchi ransomware. Per ora la motivazione è economica

Cosa succederebbe in scenari di cyber warfare?



fanpage.it

TECNOLOGIA DISPOSITIVI APP SOFTWARE SOCIAL NETWORK

12 MAGGIO 2023 16:06

L'Italia è diventata uno dei bersagli preferiti dagli hacker, soprattutto per i nostri dati sanitari

Cosa fare?

- Dotarsi di sistemi di intelligence *mirati* per minimizzare costi di audit e migliorare analisi di rischio
- Avvicinare la parte regolatoria alle esigenze tecniche (anche temporali) della cybersecurity
- Incrementare le competenze, servono esperti cyber-security e ambito sanitario e regolatorio: servono contesti culturali e capacità tecniche

Grazie

Lorenzo Bracciale

Ricercatore (RTD-B) presso Dipartimento di Ingegneria Elettronica

lorenzo.bracciale@uniroma2.it

https://lorenzobracciale.github.io/

https://www.linkedin.com/in/lorenzo-bracciale-5628855/