CWE-CAPEC ICS/OT Special Interest Group

Wednesday, September 28, 2022

THIS MEETING IS BEING RECORDED

ICS/OT Special Interest Group Participants

1. **Aagam Shah**
2. **Aamir Khan,** Tata Power
3. **Abdelrahman Elsanose**
4. **Adam Hahn**
5. **Adrian Crespo-Ortiz,** Capgemni
6. **Ahmad Sharafi,**
7. **Albert Vartic,** OMV Petrom
8. **Alex Rodriguez**, PG&E
9. **Alfinie Bullock,**
10. **Amanda Kraus**
11. **Andres Fuentes-Fernandez,** Inetum
12. **Andrew Kling**, Schneider Electric
13. **Andy Kling,** Schneider Electric
14. **Anjel Jimenez**
15. **Anton Shipulin**
16. **Armada Sramek**
17. **Ashley McGlone,** Tanium
18. **Aw Landgraaf,**
19. **Ayman Alissa**, Mckinsey
19. **Barry Greene**, Senki
20. **Bayard Johnson**
21. **Bill Newhouse**
22. **Brandon Carter**,
23. **Ben Deering,** ODNI
24. **Ben Sooter**, EPRI
25. **Beverly Novak**, INL
26. **Bill Aubin,** Nozomi Networks
27. **Bill Kintz**, Invictus
28. **Bill Newhouse**
29. **Bob Hanson,** LLNL
30. **Bob Heinemann**,
31. **Bob Radvanovsky**
32. **Bradley Nickens**, GE
33. **Bryan Beckman,** INL
34. **Bryan Owen**, Aveva
35. **Cameron Burden,**
36. **Carl Mccants,** ODNI

ICS/OT Special Interest Group Participants

37. **Carmen Zapata**, DHS
38. **Chris Charpentier**, GE
39. **Christopher Havey,** Applied Cybersecurity Engineering
40. **Christopher Sundberg**, Woodward
41. **Chris Humphrey**, Boeing
42. **Chris Levendis**,
43. **CJ Harvey,**
44. **Cody Kieltyka**,
45. **Craig Barrett,** Kinder Morgan
46. **Curtis Taylor**, CyManII
47. **Curt Wiggins**
48. **Cynthia Hsu,** DOE
49. **Dana Thomas**
50. **Dan Bennett,** NREL
51. **Dan Ehrenreich,** SCCE
52. **Danielle Jablanski**,
53. **Daniel Santos**, Forescout
54. **Daniel Stachan**
55. **Daryl Haegley**
56. **Dave Halla**
57. **Dave Keppler**
58. **David Hernandez**
59. **David Nicol**, UIUC & CyManII
60. **David Simpson**
61. **Deborah Kobza,** IACI
62. **Derek Hart**
63. **Dimple Shah**
64. **Dylan Sundy**
65. **Ed Hicks**
66. **Edward Liebig**
67. **Eric Cosman**
68. **Eric Mitchell,** NSA
69. **Eric Strief,** John Deere
70. **Erik Hrin**
71. **Espen Endal,** KraftCERT
72. **Evgeni Sabev**
73. **Gananand G Kini**
74. **Greg Ahira,** GE
75. **Greg Bastien**

ICS/OT Special Interest Group Participants

76. **Greg Sanchez**
77. **Gus Serino**
78. **Hadeli Hadeli,** Hitachi Energy
79. **Haritha Srinivasan,** FM Global
80. **Harry Perper,** Cyber Architecture and Resiliency
81. **Howard Grimes,** CyManII
82. **Iain Deason,** DHS CISA
83. **Ismael Garcia,** NRC
84. **Jace Powell,** Fortress
85. **Jarvis Robinson**
86. **Jason Li,** TrustedST
87. **Jason Plant**
88. **Jason Robbins,** AT&T
89. **Jay Gazlay,** DHS CISA
90. **Jen Walker,** Water ISAC
91. **Jennifer Pedersen**
92. **Jeremy Mckeown**
93. **Jesper Johansson,** Nouryon
94. **Jess Smith,** PNNL
95. **Jodi Jensen**
96. **Joe Agres,** West Yost
97. **Joe McCormick**
98. **Joe Weiss**
99. **John Almlof**
100. **John Kingsley**
101. **John Repici**
102. **John Schneider**
103. **John Parmley,** Zuuliot
104. **John Ransom**
105. **Jon Terrell,** Hitachi Energy
106. **Jon White,** NREL
107. **Jonti Talukdar,** Duke
108. **Jordon Sims**
109. **Jose Jimenez,** Sothis
110. **Jose Perez,** Tenable
111. **Joseph Cummings,** NYPA
112. **Joseph Januszewski,** E-Isac
113. **Joseph Matthews**

ICS/OT Special Interest Group Participants

114. **Jude Desti,** Boeing
115. **Junya Fujita**,
116. **Justin Cain**
117. **Karen Wetzel**
118. **Ken Wang,** DOD
119. **Ken Cole**, Entergy
120. **Kerry Stuver,** GE
121. **Khalid Ansari,** FM Approvals
122. **Kimberly Denbow,**
123. **Krystel Castillo**
124. **Kumar**
125. **Kyle Hussey**
126. **Kyle Johnson,** GSOC
127. **Lindsey Cerkovnik,** DHS CISA
128. **Manoj Balachandran**
129. **Marc Sachs,** Auburn University
130. **Marco Ayala**
131. **Mark Sullivan,** NSA
132. **Martijn Jansen,** Taqa
133. **Martin Kihiko**
134. **Martin Ring,** Bosch
135. **Martin Scheu,** Switch
136. **Marty Edwards**
137. **Matt Bishop,** UC Davis & CyManII
138. **Matt Sexton,** Hexagon
139. **Marie Stanley Collins**
140. **Matthew Bohne**
141. **Matthew Knoll,** ArcelorMittal
142. **Max Wandera,** Eaton
143. **Megan Samford**
144. **Melissa Vice,** Air Force
145. **Michael Chaney,** CyManII
146. **Michael Hok,** Hitachi Energy
147. **Michael Toecker**
148. **Michalis Pavlidis,** University of Brighton
149. **Mina Todorova**
150. **Monika Akbar,** UTEP & CyManII
151. **Muhammed Shaban**
152. **Nik Urlaub**

ICS/OT Special Interest Group Participants

153. **Niyu Ogunniyi,** Corteva
154. **Oystein Brekk-Saunderud,** Norma Cyber
155. **Patrick Dale**
156. **Patrick Obruba**
157. **Patti Escatel,** DHS CISA
158. **Paul Martyak,** EPRI
159. **Paul Peix,** Headmind
160. **Paul Zawada**
161. **Pete Tseronis**
162. **Peter Colombo**
163. **Peter Jackson,** SGS
164. **Peter Pongracz** (Added)
165. **Philip Huff, UALR**
166. **Pierre Janse van Rensburg,** BBA
167. **Piotr Pedziwiatr,** Arcelor Mittal
168. **Ralph Ley**
169. **Raymond Savarda**
170. **Renan**
171. **Rex Wempen,** DOE
172. **Rezaur Rahman**
173. **Rich Piazza**
174. **Richard Robinson,** Cynalytica
175. **Rita Ann Foster**
176. **Robert Garry,** GE Gas Power
177. **Robert Heinemann**, MITRE
178. **Robert Murphy**
179. **"Rob"** (Added – Unsure which of the above)
180. **Roger Johnson,** Novelis
181. **Ronald Atwater**
182. **Ryan Bays,** PNNL
183. **Ryan Gagliastre,** HF Sinclair
184. **Sabri Khemissa**
185. **Sachin Shah,** Armis
186. **Saleh Almaghrabi**
187. **Salman Salman,** Aerospace Corporation
188. **Sam Thom**
189. **Samuel Chanoski,** INL

ICS/OT Special Interest Group Participants

190. **Sandeep Shukla,** Virginia Tech
191. **Sarah Fluchs,** Admeritia
192. **Shane Stailey**
193. **Shannon Hughes**
194. **Shadya Maldonado,** Sandia
195. **Sharin Crane,** Boeing
196. **Sharla Artz**
197. **Sherry Hunyadi**
198. **Steve Battista**
199. **Steve Chapin**
200. **Steve Granda,** NREL
201. **Stephanie Saravia**
202. **Stephen Trachian,** Hitachi Energy
203. **Susan Farrell**, ObjectSecurity
204. **Ted Wittmer**
205. **Thomas Ruoff,** DHS CISA
206. **Timothy Isaacs,** NuScale Power
207. **Todd Riley, Goodyear**
208. **Tom McGoogan**
209. **Tony Turner,** Fortress
210. **Tonya Riley,** Cyberscoop
211. **Tracy Briggs,** CyManII
212. **Travis Ashley,** PNNL
213. **Vivek Ponnada**
214. **Wayne Austad,** CyManII
215. **Wayne Cantrell**
216. **William Kintz** (Added)
217. **William Welch**
218. **Yasoda Ramchune,** Chevron
219. **Zachary Rogan,** Xage

ICS/OT Special Interest Group Leadership and Support

1. **Aeriel Lane, Nexight Group**
2. **Alec Summers,** MITRE
3. **Andrew Kresses,** Nexight Group
4. **Cheri Caddy,** DOE-CESER
5. **Daisyareli Martin,** Nexight Group
6. **Greg Kerr,** Nexight Group
7. **Greg Shannon,** CyManII
8. **Ginger Wright,** INL
9. **Jeff Hahn,** INL
10. **Jeff Mitchell,** INL
11. **Jennifer Ekperigin,** Nexight Group
12. **Katie Baker,** Nexight Group
13. **Karsten Daponte,** Nexight Group
14. **Lindsay Kishter,** Nexight Group
15. **Stephen Bolotin,** Nexight Group
16. **Steve Christey,** MITRE

Agenda

Eastern Time	Activity
3:00 – 3:05 pm	**Login and Roll Call**
3:05 – 3:10 pm	**Opening Remarks** • Review meeting objectives • Review material covered in last meeting
3:10 – 3:25 pm	**CWE and CAPEC Updates Related to ICS/OT Weaknesses** • CWE 4.9 updates • CAPEC 3.8 updates • Enhancements to CWE website
3:25 – 3:45 pm	**Kicking Off "Boosting" and "Mapping" Sub-Working Groups** • Howard Grimes (co-chair) to present "Boosting CWE Content" subgroup plans • Bryan Owen (co-chair) to present "Mapping CWE to 62443" subgroup plans • Solicit additional volunteers • Open Q&A
3:45 – 3:55 pm	**Coordinate Additional Outreach Needed for Sub-Working Groups** • Discuss analysis of current subgroup volunteers • Coordinate outreach to additional participants as needed
3:55 – 4:00 pm	**Wrap-Up** • Closing remarks • Next SIG meeting – Wed 11/30 @ 3pm • Action Items
4:00 pm	**Meeting Ends**

Opening Remarks

Opening Remarks

Meeting Objectives

1. Review CWE 4.9 and CAPEC 3.8 updates related to ICS/OT weaknesses
2. Prepare to kickoff "Boosting" and "Mapping" sub-working groups
3. Coordinate any additional outreach needed for sub-working groups

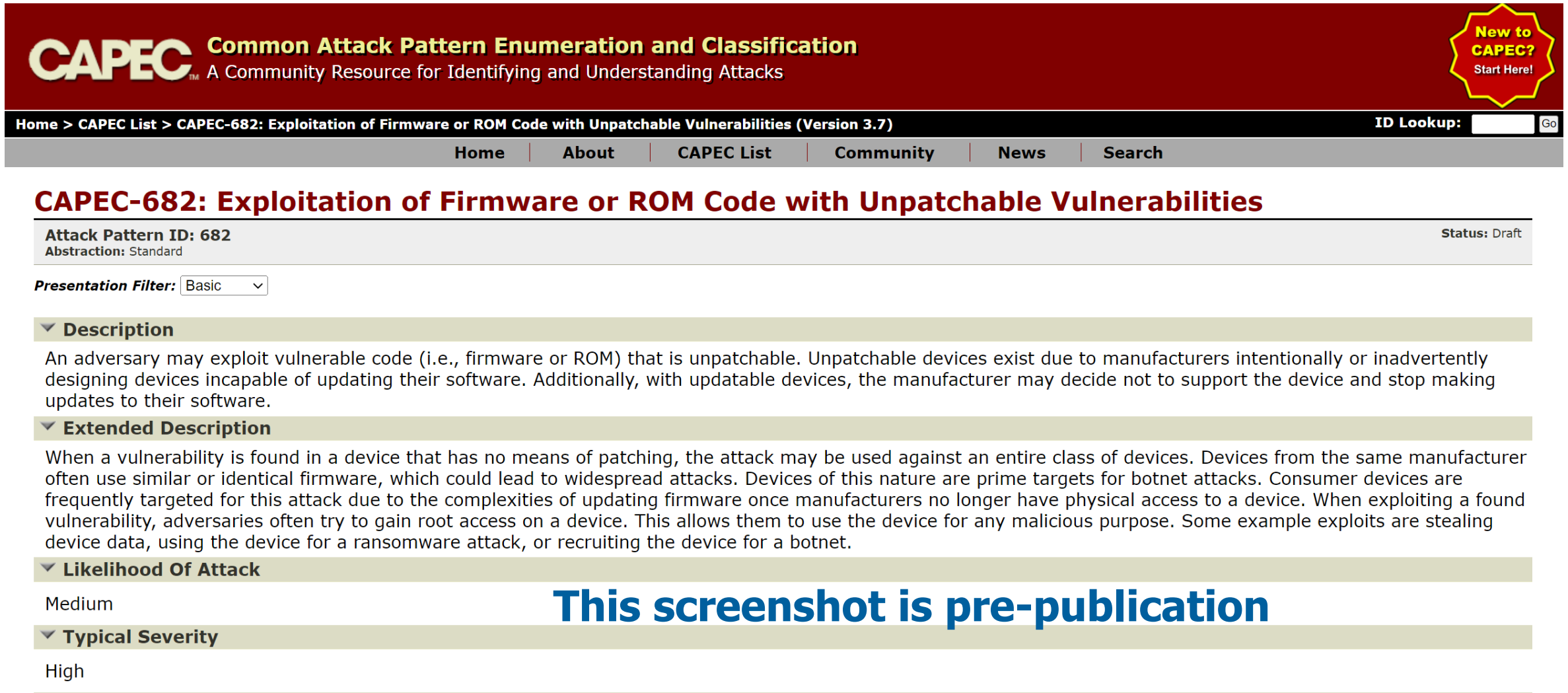
Review of Last Meeting 8/31

- Discussed how SIG participants use CWE today
  - To enable comparison of security product capabilities
  - To help with development
  - Conducting larger scale analysis and trend analysis
  - To "get in front of the problem" rather than waiting to respond to vulnerability discovery in OT systems
- Discussed how SIG participants would like to use CWE in the future
  - To support/incorporate Cyber Informed Engineering (CIE) from the original Securing Energy Infrastructure Executive Task Force
  - To prioritize response to threat intel given limited resources
  - To enable proactive guidance on where vulnerabilities may be
  - To map against risk scoring and quantify presence of risk
  - To prioritize and improve efficacy of mitigations (identified as longer-term goal for both CWE and CAPEC by MITRE)
  - To improve efficiency in mitigation, prevention, and response to threats
- Identified, structured, and determined next steps for "Boosting" and "Mapping" subgroups
- Enumerated the set of stakeholders that need to be involved in the SIG

CWE/CAPEC: Upcoming Releases

CAPEC 3.8 Release Highlights for ICS/OT SIG – Thursday, September 29

- **Multiple new attack patterns potentially related to ICS/OT**
- **CAPEC-694: System Location Discovery (discover geographical location)**
- **CAPEC-696: DHCP Spoofing**
- **Software supply chain**
  - CAPEC-695: Repo Jacking (adversary re-registers a repository whose location changed)
  - CAPEC-693: StarJacking (make a software package seem popular)
  - CAPEC-690: Metadata Spoofing (make software repositories seem legitimate and trusted)
- **CAPEC-682: Exploitation of Firmware or ROM Code with Unpatchable Vulnerabilities**
- **… and others**



CAPEC Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

New to CAPEC? Start Here!

Home > CAPEC List > CAPEC-682: Exploitation of Firmware or ROM Code with Unpatchable Vulnerabilities (Version 3.7)

ID Lookup: Go

Home | About | CAPEC List | Community | News | Search

CAPEC-682: Exploitation of Firmware or ROM Code with Unpatchable Vulnerabilities

Attack Pattern ID: 682
Abstraction: Standard

Status: Draft

Presentation Filter: Basic

Description

An adversary may exploit vulnerable code (i.e., firmware or ROM) that is unpatchable. Unpatchable devices exist due to manufacturers intentionally or inadvertently designing devices incapable of updating their software. Additionally, with updatable devices, the manufacturer may decide not to support the device and stop making updates to their software.

Extended Description

When a vulnerability is found in a device that has no means of patching, the attack may be used against an entire class of devices. Devices from the same manufacturer often use similar or identical firmware, which could lead to widespread attacks. Devices of this nature are prime targets for botnet attacks. Consumer devices are frequently targeted for this attack due to the complexities of updating firmware once manufacturers no longer have physical access to a device. When exploiting a found vulnerability, adversaries often try to gain root access on a device. This allows them to use the device for any malicious purpose. Some example exploits are stealing device data, using the device for a ransomware attack, or recruiting the device for a botnet.

Likelihood Of Attack

Medium

This screenshot is pre-publication

Typical Severity

High

CWE 4.9 Release Highlights for ICS/OT SIG – October 13, 2022

- **New CWE-1389: Improper Conversion of Numbers with Different Radices**
  - Known to cause incorrect IP addresses/ranges to be used
- **Some entries updated to indicate they are found in ICS/OT Technology**
  - CWE-798: Hard-Coded Credentials, CWE-306: Missing Authentication, others
- **Observed examples (CVEs) from the OT:ICEFALL disclosures**
  - PLC, DCS, RTU, others
- **Web site will allow customized views of certain fields**
  - Theoretical, Operational, Mapping-Friendly, Complete
- **Mapping notes will discourage use of high-level CWEs**
  - More detailed CWEs improve trend analysis and are more actionable
- **Late October? Draft of CWE Scope Exclusions**
  - Direct relationships with some categories in CWE-1358 view (Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS)

Example Change – CWE-798: Hard-Coded Credentials

CWE-798: Use of Hard-coded Credentials

Weakness ID: 798
Abstraction: Base
Structure: Simple

View customized information: Theoretical | Operational | Mapping-Friendly | **Complete**

change →

Description

The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.

Applicable Platforms

Languages

Class: Language-Independent *(Undetermined Prevalence)*

Technologies

Class: Mobile *(Undetermined Prevalence)*

Class: ICS/OT *(Often Prevalent)*

References

[REF-7] Michael Howard and David LeBlanc. "Writing Secure Code". Chapter 8, "Key Management Issues" Page 272. 2nd Edition. Microsoft Press. 2002-12-04. <https://www.microsoftpressstore.com/store/writing-secure-code-9780735617223>.

[REF-729] Johannes Ullrich. "Top 25 Series - Rank 11 - Hardcoded Credentials". SANS Software Security Institute. 2010-03-10. <http://blogs.sans.org/appsecstreetfighter/2010/03/10/top-25-series-rank-11-hardcoded-credentials/>.

[REF-172] Chris Wysopal. "Mobile App Top 10 List". 2010-12-13. <http://www.veracode.com/blog/2010/12/mobile-app-top-10-list/>.

[REF-962] Object Management Group (OMG). "Automated Source Code Security Measure (ASCSM)". ASCSM-CWE-798. 2016-01. <http://www.omg.org/spec/ASCSM/1.0/>.

[REF-1283] Forescout Vedere Labs. "OT:ICEFALL: The legacy of "insecure by design" and its implications for certifications and risk management". 2022-06-20. <https://www.forescout.com/resources/ot-icefall-report/>.

Example Change (2) – CWE-798: Hard-Coded Credentials

```
</connectionStrings>
...
```

Username and password information should not be included in a configuration file or a properties file in cleartext as this will allow anyone who can read the file access to the resource. If possible, encrypt this information.

Example 5

In 2022, the OT:ICEFALL study examined products by 10 different Operational Technology (OT) vendors. The researchers reported 56 vulnerabilities and said that the products were "insecure by design" [REF-1283]. If exploited, these vulnerabilities often allowed adversaries to change how the products operated, ranging from denial of service to changing the code that the products executed. Since these products were often used in industries such as power, electrical, water, and others, there could even be safety implications.

Multiple vendors used hard-coded credentials in their OT products.

Observed Examples

Reference	Description
CVE-2022-29953	Condition Monitor firmware has a maintenance interface with hard-coded credentials
CVE-2022-29964	Distributed Control System (DCS) has hard-coded passwords for local shell access
CVE-2022-30997	Programmable Logic Controller (PLC) has a maintenance service that uses undocumented, hard-coded credentials
CVE-2022-30314	Firmware for a Safety Instrumented System (SIS) has hard-coded credentials for access to boot configuration
CVE-2010-2772	SCADA system uses a hard-coded password to protect back-end database containing authorization information, exploited by Stuxnet worm
CVE-2010-2073	FTP server library uses hard-coded usernames and passwords for three default accounts
CVE-2010-1573	Chain: Router firmware uses hard-coded username and password for access to debug functionality, which can be used to execute arbitrary code
CVE-2008-2369	Server uses hard-coded authentication key

"Boosting CWE Content" Subgroup

#1 - Boosting CWE Content

VOLUNTEERS	
Co-Chairs	**12.** Bryan Owen
1. Howard Grimes	**13.** Gus Serino
2. John Kingsley	**14.** Beverly Novak
	15. Joseph Januszewski
Participants	**16.** Ryan Bays
1. Evgeni Sabev	**17.** Wayne Austad
2. Oystein Brekke-Sanderud	**18.** Monika Akbar
3. Paul Peix	**19.** Adrian Crespo
4. Iain Deason	**20.** Steve Christey Coley
5. Marco Ayala	**21.** David Hernandez
6. Melissa Vice	**22.**
7. Junya Fujita	**23.**
8. Kyle Hussey	**24.**
9. Edward Liebig	**25.**
10. Ismael Garcia	
11. Mike Chaney	

Logistics

- Kickoff meeting scheduled for **Wednesday 10/12 from 10:30 – 11:30 am ET**
- Meeting biweekly

Immediate Tasking

1. Expand participants with outreach to manufacturers
2. Conduct deeper analysis of 20 categories of security vulnerabilities developed by the SEI ETF. ICS/OT experts need to evaluate if current mappings to CWE are accurate and if there are additional opportunities to expand CWE content
3. Nominate existing CVEs for ICS/OT issues that CWE does not have coverage for
4. Examine common architectural weaknesses in ICS/OT/SCADA
5. Examine Icefall. Existing CWEs out there but may not be findable/understandable for ICS/OT. May involve additional content in CWEs to labeled as explicitly for ICS/OT. (in progress at MITRE)
6. Wrestle with scope questions. It may be important or useful to expand CWE's scope to include those things. May produce certain proposals. If not part of CWE, how do we represent them in ways to make them more accessible to ICS manufacturers and practitioners?

"Mapping CWE to 62443" Subgroup

#3 – Mapping CWE to 62443

VOLUNTEERS	
Co-Chairs	**13.** Stephen Trachian
1. Khalid Ansari	**14.** Christopher Sundberg
2. Bryan Owen	**15.** Beverly Novak
	16. Jose Luis Jimenez
Participants	**17.** Curtis Taylor
1. Oystein Brekke-Sanderud	**18.** Mike Chaney
2. Paul Peix	**19.** Mina Todorova
3. Marco Ayala	**20.** John Kingsley
4. Martin Scheu	**21.** Adrian Crespo
5. Melissa Vice	**22.** Alec Summers
6. Matt Knoll	**23.** Richard Robinson
7. Junya Fujita	**24.** Michael Thompson
8. Kyle Hussey	**25.**
9. Edward Liebig	**26.**
10. Ismael Garcia	**27.**
11. Sam Chanoski	
12. Susan Farrell	

Logistics

- Kickoff meeting scheduled for **Tuesday 10/11 from 1 – 2 pm ET**
- Meeting biweekly

Value Proposition

- ICS-ify CWE/CAPEC by referring to 62443 requirements/guidance, especially where OT guidance differs from IT

Immediate Tasking

1. Tier ISA/IEC 62443 requirements (must have, nice to have, if there is time) as candidates to enrich CWE/CAPEC
2. Identify failure examples to be referenced in applicable CWE(s)/CAPEC(s)
3. Provide recommendations to CWE/CAPEC to add cross references to ISA/IEC 62443 requirements/guidance based including the example case(s)

Deliverables

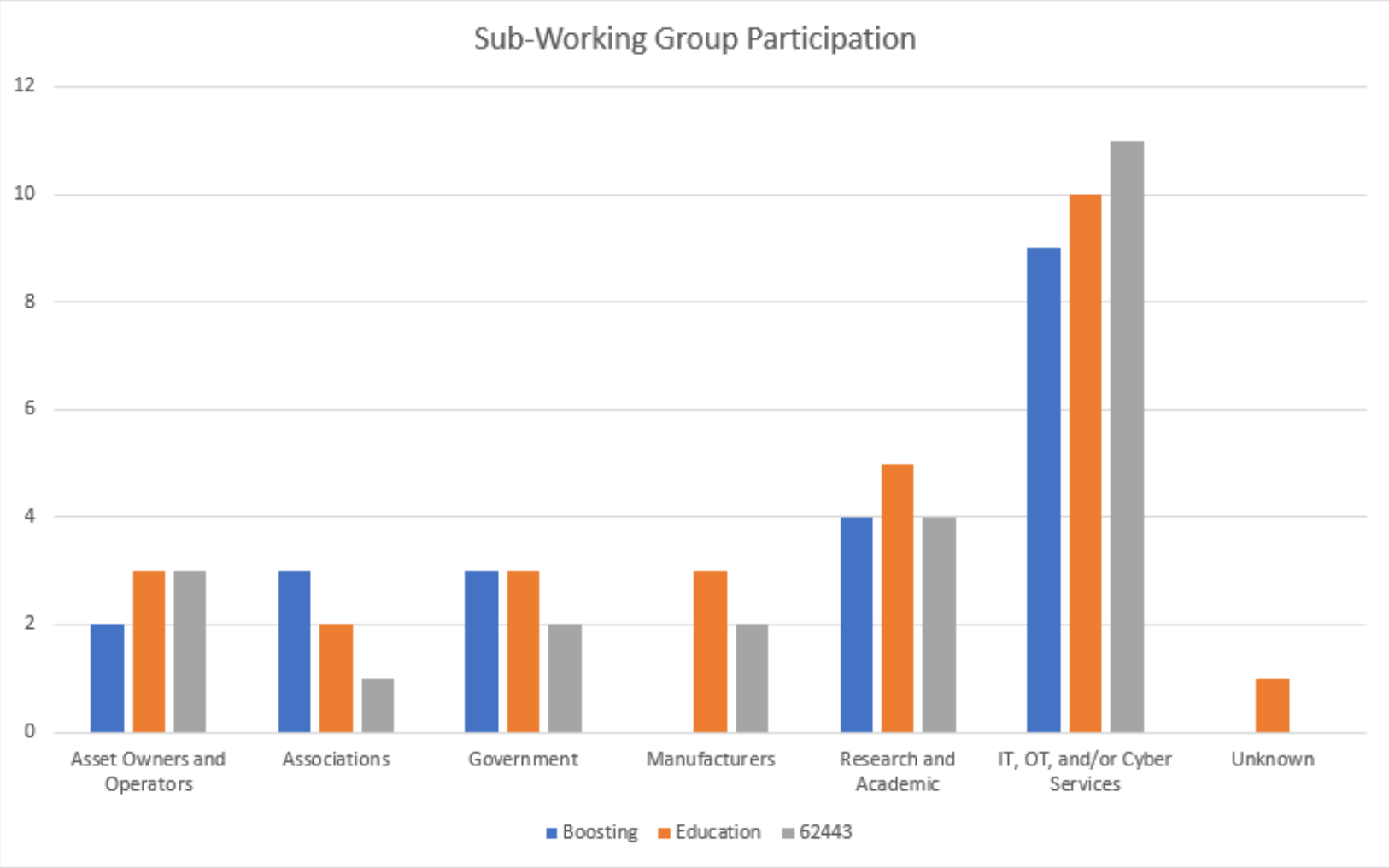
1. The mapping itself in the CWE's Taxonomy Mapping elements.
   - Mapping should be integrated into the definition of CWE instead of having a separate reference tool.
2. Another deliverable could be recommendations to ISA/IEC 62443 committees to address CWE's that are not currently addressed in the standards, etc. (which is mentioned under work plan).

Subgroup Discussion Questions

- **Is it appropriate that the "Boosting" and "Mapping" subgroups are scoped explicitly around CWE and not CAPEC?**
  - Do more explicit connections need to be draw to CAPEC now or at a future date?
- **For the "Mapping" subgroup:**
  - Does this mapping example make sense?
    - CWE-862 is *Missing Authorization* and its description states: "The software does not perform an authorization check when an actor attempts to access a resource or perform an action."
    - Requirement CR 2.1 of 62443-4-2 states: "Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities."
    - 62443-4-2 CR 2.1 → CWE-862
    - In cases where CWEs are not address by 62443 product requirements, look at broader, non-product requirements such as network segmentation and map those. CWEs would then be shared with ISA99 committees for addressing more specifically.
  - Should this subgroup look at all the current 900+ CWEs or only the 20 ICS-specific ones developed by the SEI ETF and CyManII?
- **Any other general questions?**

Coordinate Additional Outreach Needed for Sub-Working Groups

Analysis of Subgroup Participation



Outreach next steps

- **Solicit additional participants via ICS/OT SIG listserv**
  - Leverage the SIG slicksheet (1pg front & back) and updated charters
- **Promote subgroups on social media**
  - Welcome promotion on LinkedIn or other recommended outlets
- **Greg Shannon reaching out to GRF to court**
  - Electricity Information Sharing and Analysis Center (E-ISAC)
  - Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC)
  - Other Manufacturing Innovation Institutes (MIIs)
- ***What else?***

Wrap-Up

Major Milestones

- **CWE-CAPEC board meeting**
  - Tomorrow 9/29 @ 3:15 pm
- **Sub-Working Groups meet bi-weekly**
  - Mapping to 62443 Tuesday 10/11 from 1:00 to 2:00pm ET
  - Boosting CWE Content Wednesday 10/12 from 10:30 to 11:30am ET
- **ICS/OT SIG meets bimonthly going forward**
  - Next meeting Wednesday 11/30 from 3:00 to 4:30pm ET
- **CWE/CAPEC publish content on quarterly basis**
  - CWE 4.9 – Thu 10/13
  - Next major update for CWE 4.10 – Jan 2023
  - CAPEC 3.8 – Thu 9/29
  - Next major update for CAPEC 3.9 – Jan 2023 (less certain)

Action Items

1. **If you have not done so already, please reach out to sign-up for the sub-working groups.**

MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org