Investigación de Vulnerabilidades en Sistemas SCADA.

Eduardo Vásquez P.; Helder Castrillón C.

Vulnerabilidad	Título	Referencia	¿Asociado a subestaciones eléctricas?
Denial-of-Service	Simulation and Impact Analysis of Denial-of-Service Attacks on Power SCADA	[1]	No
Default Credentials, Unsupported Unix operating system, SQL Injections, OpenSSH vulnerabilities, Buffer Overflows, DoS, XSS, Browsable Web Directories, Modbus coil access, Cleartext submission of credentials, authentication without HTTPS, Generic paramater injections, web mirroring	Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques	[2]	No
Replay Attack, Man-in-the-Middle Attack, Brute Force Attack, Dictionary Attack, Eavesdropping, Denial-of-Service Attacks, War Dialing, Default Passwords, Data Modification	Securing Communications for SCADA and Critical Industrial Systems	[3]	No
Architectural Vulnerabilities, Security Policy Vulnerabilities, Software and Hardware Vulnerabilities, Communication Protocol Vulnerabilities	Security of SCADA Systems Against Cyber–Physical Attacks	[4]	Sí (mencionado)
Man-In-The-Middle (MITM) Attack, DoS (Denial of Service) Attack, Replay Attack, Injection Attack, Spoofing Attack, Eavesdropping, Modification, Reconnaissance Attack	Review on Cyber Vulnerabilities of Communication Protocols in Industrial Control Systems	[5]	Sí
Source code design and implementation, Buffer Overflow, SQL Injection, Cross Site Scripting (XSS), Effective patch management application	An Overview of Cyber-Attack Vectors on SCADA Systems	[6]	No
APT (Advanced persistent Attack)	APT Attack Analysis in SCADA Systems	[7]	No
Improper input validation, Buffer overflow, Command injection and Cross-site scripting, Poor code quality, Improper control of a resource, Feeble access control mechanism, Poor authentication, Cryptographic Issues, Poor credential management and maintenance practices, Inadequate policies & procedures, Network Design Fragility, Feeble Firewall, Audit and accountabilities Rules	SCADA (Supervisory Control and Data Acquisition) Systems: Vulnerability Assessment and Security Recommendations	[8]	No

Referencias

[1] R. Kalluri, L. Mahendra, R. K. S. Kumar, and G. L. G. Prasad, "Simulation and impact analysis of denial-of-service attacks on power SCADA," *2016 Natl. Power Syst. Conf. NPSC 2016*, no. 1, 2017, doi: 10.1109/NPSC.2016.7858908.

[2] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," *IEEE Int. Conf. Intell. Secur. Informatics Cybersecurity Big Data, ISI 2016*, pp. 25–30, 2016, doi: 10.1109/ISI.2016.7745438.

[3] T. Bartman and K. Carson, "Securing communications for SCADA and critical industrial systems," *69th Annu. Conf. Prot. Relay Eng. CPRE 2016*, 2017, doi: 10.1109/CPRE.2016.7914914.

[4] V. L. Do, L. Fillatre, U. Côte, S. Antipolis, I. Nikiforov, and U. De Technologie, "Security of SCADA Systems Against Cyber – Physical Attacks," no. 10, 2017.

[5] S. Dorqj, Z. Vhyhudo, W. S. Dwwdfnv, and D. Q. G. Frxqwhuphdvxuhv, "Review on Cyber Vulnerabilities of Communication Protocols in Industrial Control Systems," vol. 4, no. 1, pp. 1–6, 2015.

[6] E. Irmak and I. Erkek, "An overview of cyber-attack vectors on SCADA systems," *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/ISDFS.2018.8355379.

[7] X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, and W. Zhang, "APT attack analysis in SCADA systems," *MATEC Web Conf.*, vol. 173, pp. 2–6, 2018, doi: 10.1051/matecconf/201817301010.

[8] D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Secur.*, vol. 89, p. 101666, 2020, doi: 10.1016/j.cose.2019.101666.