Demo Company
Security Assessment Findings Report

Date: November 19th, 2022

Contact Information

Name	Title	Contact Information
NUWE x Schneider Electric		
Onofre Carmelo Bustos Gimeno	obustosgimeno9fc3b3e84b9d9fcd	Email: obustosgimeno@gmail.com Github: el-kiosquet
Pablo Picó Silvestre	picosilvestrepablo	Email: picosilvestrepablo@gmail.com Github:
Felipe Bastante Flor	fbastantef	Email: fbastantef@gmail.com Github:
Name	Participant	Email: Github:

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
Security Audit	Machine IP

Security Audit Findings

Reverse shell – /vese-projects-code/websites/php/test_comment.php (Critical)

Description:	A reverse shell has been found on the referenced path, which gives access to the complete system when contact form is filled by the attacker with the following credentials: Name = “test1” Email = test@test.com Message = “test2” The IP of the attacker is “158.46.250.151” and connects to the port 9001.
Impact:	Critical
System:	18.170.23.70
References:	

Exploitation Proof of Concept

Remediation

Who:	IT Team
Vector:	Remote
Action:	Item 1: Remove the instruction “eval()” in line 20 of the file “test_comment.php”. Item 2: Find how the code has been modified. Item 3: Item 4: Additional Recommendations: With the IP of the attacker, legal actions can be taken. The system has been compromised. The users should be informed.

Exploitation Paths

Security Audit Findings

SQL injection – /vese-projects-code/websites/php/login.php (Critical)

Description:	SQL injections because of the missuse of the function “addslashes()”, code can be introduced through login attempt.
Impact:	Critical
System:	18.170.23.70
References:	

Exploitation Proof of Concept

Remediation

Who:	IT Team
Vector:	Remote
Action:	Item 1: The fuction “addslashes()” can’t be used for sanitizing passwords in SQL Item 2: Change the function “addslashes()” for My_SQL function “mysql_real_escape()” Item 3: Item 4: Additional Recommendations:

Suspected vulnerabilities:

The passwords are codified with MD5, which could lead to hash collisions, that means that two different passwords can have the same hash.

References: https://en.wikipedia.org/wiki/MD5

https://en.wikipedia.org/wiki/Hash_collision