Security Advisory Report - OBSO-1404-01

OpenScape Deployment Service - Blind SQL Injection Vulnerability (CVE-2014-2652)

Creation Date: 2014-04-11
Last Update: 2014-04-11

Summary

The OpenScape Deployment Service (DLS) before V7 R1.11.3 is vulnerable to a time-based blind SQL injection that could allow remote attackers to perform unvalidated queries on the database and potentially run commands on the server.

The risk is rated **medium.**

Vulnerability Details

The vulnerability is due to insufficient input validation at the DLS Graphical User Interface (GUI - https port 10443). This may allow unauthorized attackers to extract contents from the DLS database, alter it or potentially execute commands on the DLS server.

CVSS Scores:

- Base Score 6.6, Temporal Score 5.7
  (AV:N/AC:H/Au:N/C:P/I:C/A:P/E:H/RL:OF/RC:C)

Mitre (cve.mitre.org) has assigned the id CVE-2014-2652 to this issue.

Affected Products

- OpenScape Deployment Service V6 and V7 (before V7 R1.11.3)

Recommended Actions

Install the following hotfix release (or later versions) of OpenScape Deployment Service:

- V7 R1.11.3, release date: 2014-03-28

General recommendation: evaluate the possibility to limit access to the DLS GUI for authorized administrator devices only. This adds an additional layer of security by reducing the attack surface on the DLS server.

References

CVE ID: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2652

Revision History

2014-04-11: Initial release

Advisory ID: OBSO-1404-01 (a=75), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com