Security Advisory Report - OBSO-1401-04

OpenScape Deployment Service - SQL Injection Vulnerability

Creation Date: 2014-01-31  
Last Update: 2014-01-31

Summary

OpenScape Deployment Service (DLS) contains a vulnerability that could allow an authenticated attacker to access, create or modify any information in the DLS database.

The risk is rated high (CVSS Base Score: 8.5).

Vulnerability Details

This vulnerability is due to improper validation of DLS client requests by the DLS server application. An attacker who has successfully authenticated against the DLS (by using any account, regardless of this account's access rights in the DLS application) could exploit this vulnerability by injecting arbitrary Structured Query Language (SQL) commands. This allows the attacker to get complete administrative control of the DLS server application.

Affected Products

- OpenScape Deployment Service, all versions

Recommended Actions

Upgrade OpenScape Deployment Service to V7 R1.7.1 (released: 2013-07-19) or any later version of V7 R1.

Recommended mitigation measures for existing installations:

- Review the list of user accounts with access to the DLS application. Ensure that appropriately secured passwords are set (follow the password policy recommendations in the product Security Checklist of OpenScape DLS V7).  
- Restrict the access to DLS ports 10443 (Web-GUI) and 10444 (DLS-API) by appropriate firewall rules and/or IP address-based Access control lists.

References

N.A.

Revision History

2014-01-31: Initial release