



Security Advisory Report - OBSO-1306-02

OpenStage Cloud Diagnostic Data Collector - PHP and Web Server Vulnerabilities (CVE-2013-1643, CVE-2012-3499)

Creation Date: 2013-06-17
Last Update: 2013-06-17

Summary

OpenStage Cloud Diagnostic Data Collector (Cloud-DDC) V1 R4 is released to address security vulnerabilities in the components PHP and Apache HTTP server. The vulnerabilities are rated as "medium" in the context of Cloud-DDC.

Customers are advised to perform the "Recommended Actions" at the earliest opportunity.

Vulnerability Details

Cloud-DDC is affected by the following vulnerabilities:

- **CVE-2013-1643**: A vulnerability in the SOAP parser in PHP allows remote attackers to read arbitrary files from the Cloud-DDC server.
- **CVE-2012-3499**: The Apache HTTP server of Cloud-DDC is vulnerable to cross-site scripting (XSS) attacks due to unescaped hostnames and URIs HTML output.

Refer to the references given below for more details.

Note that Cloud-DDC is not affected by other vulnerabilities, as recently reported for PHP or Apache HTTP Server. This includes CVE-2013-1635, CVE-2013-2110 (PHP) and CVE-2012-4558 (HTTP Server).

Affected Products

- OpenStage Cloud Diagnostic Data Collector V1

Recommended Actions

Upgrade to **OpenStage Cloud Diagnostic Data Collector V1 R4.0.0** to address these vulnerabilities. For details refer to the Release Note of Cloud-DDC V1 R4.0.0 (release date: 2013-06-13).

References

PHP:

- Release note for PHP 5.3.23: <http://php.net/archive/2013.php#id2013-03-14-1>

Apache:

- Release information for HTTP Server 2.2.24: <http://www.apache.org/dist/httpd/Announcement2.2.html>

Mitre:

- CVE-2013-1643: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1643>
- CVE-2012-3499: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3499>

Revision History

2013-06-17: Initial release

Contact and Disclaimer

OpenScape Baseline Security Office

obsso@unify.com

© Unify Software and Solutions GmbH & Co. KG 2013

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

www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.