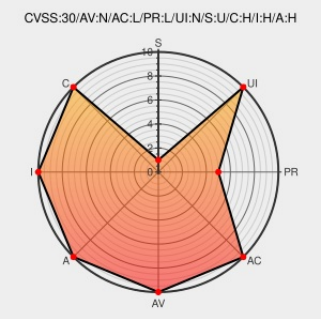
CVE-2015-8542

Published on: 12/15/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8542

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ox Guard from Open-xchange contain the following vulnerability:

An issue was discovered in Open-Xchange Guard before 2.2.0-rev8. The "getprivkeybyid" API call is used to download a PGP Private Key for a specific user after providing authentication credentials. Clients provide the "id" and "cid" parameter to specify the current user by its user- and context-ID. The "auth" parameter contains a hashed password string which gets created by the client by asking the user to enter his or her OX Guard password. This parameter is used as single point of authentication when accessing PGP Private Keys. In case a user has set the same password as another user, it is possible to download another user's PGP Private Key by iterating the "id" and "cid" parameters. This kind of attack would also be able by brute-forcing login credentials, but since the "id" and "cid" parameters are sequential they are much easier to predict than a user's login name. At the same time, there are some obvious insecure standard passwords that are widely used. A attacker could send the hashed representation of typically weak passwords and randomly fetch Private Key of matching accounts. The attack can be executed by both internal users and "guests" which use the external mail reader.

CVE-2015-8542 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20160302 Open-Xchange Security Advisory 2016-03-02
Open-Xchange Guard 2.2.0 / 2.0 Private Key Disclosure ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	CONFIRM packetstormsecurity.com/files/136069/Open-Xchange-Guard-2.2.0-2.0-Private-Key-Disclosure.html
Open-Xchange Guard Access Control Flaw Lets Remote Authenticated Users Obtain Private Keys in Certain Cases - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1035174

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Open-xchange	Ox Guard	All	All	All	All

cpe:2.3:a:open-xchange:ox_guard:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report