The Faraday development team is aware that the information stored in the platform is of the highest criticality. With this in mind, we have developed this guide to perform Faraday Hardening.

SSL

Use SSL for cipher information between client and server, using a Nginx server.

More information HERE

Couchdb

CVE-2017-12636 and CVE-2017-12635

We recommend all customers upgrade to Couchdb 1.7.1 to protect against these vulnerabilities.

Admin party:

By default the Couchdb installations come without any user or password configured as administrator, this status in Couchdb is called Admin party. Any request that reaches the Couchdb APIs will have administrator user privileges exposing the service to previously mentioned exploit.

Remediation: Create an administrator user and use a secure password.

Couchdb RCE authenticated.

Couchdb has a known vulnerability that allows the execution of code remotely, as long as you have administrator privileges, in Metasploit you can look more closely at the module to take advantage of it.

Remediation:

Modify the local.ini file, usually located in /etc/couchdb/, locate the [httpd] section and add the following:

```
config_whitelist = []
```

Warning: If you are using Professional or Corporate versions, you won't be able to change the password or roles of admin users (pentesters and clients should work ok) in the Web UI. We are working in fixing this issue.

With that the _config API is totally disabled, any change of configuration to Couchdb must be done by modifying the local.ini manually. Warning: If you are going to use LDAP with Faraday, you must configure the LDAP before applying this remedy.

Dont expose the couchdb service outside if you dont need that.

Public database.

In faraday each workspace is a database, if you create a public workspace this ends up being a public database, so if your instance of couchdb is accessible externally anyone who knows the name of the workspace can access the information stored in that.

Remediation:

Do not use public workspaces.

Do not expose Futon (_utils) externally.

Report a security vulnerability in Faraday.

Send us a email with all relevant information about your discovery at:

security@faradaysec.com

To encrypt your communications, or to verify signed messages you receive from us you can use the PGP key below.

Key ID: 3A48E3A9FC5DE068 **Key type:** RSA **Key size:** 4096

Fingerprint: `841D C247 7544 1625 5533 7BC8 3A48 E3A9 FC5D E068`

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

xsFNBFkt/tgBEACTfM0cg61cs2J1WFOEEuH+BBkN19oieTv0KK0cZZmzuzut
gclFdE4gbpsPzvczcpd2Px0KqkRbI0IBjxoP2c6m94RK5mxcyIDM/C/WxCt2
9BdWrmVzI6SmNZxxYg3ThH1ccv3M76toIf5e5ylykuKGAALh/OYn/CgYvNz2
3pChfwFmzBwFLumMCjjkhmaIp5a1BZcwnv+V3LGG2YK/ORswD2rNqk7z13lE
xVdm8kASO+d+UVW8sSXPDWzeYCalG2RrJ893pX8t47q3uOSiu8i+OK1gTV9t
knTLi7AB00imPqndM6i5rItBxEPJLz5NOeFruv9nBDuWMFbbvjJ49wYVYmnD
xuu651ZS65tdZkGUybp4shvtiUX/uZVdbwu/2GP3/eE9bsMHk8OA0QgXlXuZ
06Ad3jz6zkdhFeNtalKRfoXwZgSfg/ppC8/qIG8Cat9JhaSJLOQes1Vvvmaf
db9y6C8hTUSECik1+JHziiXYREWswTl+8xwuDsILj1wJNAxsOMArf2ghH+nl
AEM/ISlsaLnIFWsSlC0ZsV3CefSXIm3Q8BYaMhO+6qJqS1MiFjf7MDETP5eh
O4Otp9GBaz3I5Hbr6rf1/NyL9vl9pckCCa1lAR1VRzLIsxH6rcUAQ7cuUqP4
V72pNKJfVk/fpGHvWeJT9OJH3h8MEyoRTRyLnQARAQABzSpTZWN1cml0eSBG
YXJhZGF5IDxzZWN1cml0eUBmYXJhZGF5c2VjLmNvbT7CwXUEEAEIACkFAlkt
/t0GCwkIBwMCCRA6SOOp/F3gaAQVCAIKAxYCAQIZAQIbAwIeAQAAWHUQAIhU
aa1Ml87DpNhk3h3Pso2eo3sdiIuuWNPQzcs+oNgnui6SrhZK8MXTYzAPRzSY
2s7rbkvLlZRgsbUx5R7DZQ6tPq0cu87NjfY4DhGnlwpZxKwwhSDqQ4FCaJLU
6jTTTb8oCrLTqx15RsYyZlV82GIAszlj/BMHLiDCaPA8SOV7gmDtAA9nRWJC
Yjiz1An4UNVKsTDFZ5/a2ZfxOh2KqwuT7gLL39DutRAV/nNQWipdPqVVJ5Ut
ZaQ/Vr6omdpsKgIyjFfAL+Yrh+9AP99PVQjq1NAAg9GtF8BQ+KKWYhqut5mD
cyFtvKpbQQywc2+njuUqpj53opaNGwCi/PIeIPmxbNq9I5Oyf2ZYS3lNeRsp
sptA7JlZSrm0enXfpONIG1stiCraayqSB0ABatroviuWNTmbvr3ogrxa4LS+
9qJAWF6fb9o1qUz9pBN8Op7CCgcFC8Wq/QwC2KTwAstqwC9nxQOc//r1DlDY
fwZJ+xoLbUA5q2Uir3eL+Jju/8vyHHDvQwtwZZe2dyEclcLHg1rCZdxrMcXr
ov8hn/MUJ+KOakLa7JTH/aQlKfA0KkulLVDLq0clhJHD7UTliPBePsntPgU+
4Wn6NbRP3FDMDY9n2ZJaHiutOsPTSy1960zCTWMKlqYhB/YmexhVvexmAcXv
```

```
SNoRZ0A+5jeXqStN/m/gzsFNBFkt/tgBEADWInjRV7lLWRvFkOknqWrl1V+U
x8WM//F2/rt5vHDM98cp7cYYVtizc/sFcLbUQWA5KcB6r51A5PMRbPzPWc8r
IFQBdlmFW7re6Qpt60RevfUJ4UcGAsVi7JKq8Mm9yu2OxEBYbofJgY2mk3QD
CV4/lZ2AKQyRSDJrKonWm/Ep/ucn4L4qRY+uWQvoIAIg+U6a7h4OEONpKq24
CPreEIr4nUu/0OqkcTUDBBbHMEsFqDPLoHmFFvsqlazqmUsJTEPn71xqME8h
GN35XIOxZGex4FCrxmQa5gyFnGTRNzdT4iI9DVoPARJhRE7rEiG5rcCktgA7
HBBJv2M90HUhM413/p2nbGm7peuPEjMnfMxzE0+3xyLKluGYQUbAmbp48Ih3
4bAWlgYGPjEyi8vNNnpmoG4yt3JbFDn8xGV9mkFrp5neN//E33quhYOIVJIF
adFePbZ8bKc2EWTpXUutds40+yFvp4ij3iKPb4u2q9+MSDlvaZZC9tY7csfr
csLsgmgLRrOkUvlo6JdVZI9OTnMKncqzMQt6ppXytAves2F+WuKuGR+0+p1B
WkV56/HfGDxuzqnhSAeFaDNzjqVbJ0/xVvH7DMvkbimV3AUPvm42mTmWwcY8
JN/YyXPh7Al6GtYCP5msZK3yGmh+FY4p+KCByxWlQUFvqux8dBFQCI7B5wAR
AQABwsFfBBgBCAATBQJZLf7fCRA6SOOp/F3gaAIbDAAASJ4P/3qiw+eOi39Y
Kz/Bzp6rVhHxa6HXCSWSAGLcQhp10ZtQbjlnnV+JCij7ZtqWEOjQgXU00Ex4
Fs2nOrIpXZ57BcBBZEIyCjhnzdcqCuu0sL2Q+BYMa0gUIa/vIPboWXyOW6mb
P9homHcXpURZzFTZ5nVnGVVwcy08Pg8Ij4gAQVdvBACn4aIToInqQT2YD8E5
ucdtuJP5uJfqHUTrU1B7UHjTxmiafSCHVDHqTRR4I6jz4qrBn2VeblHjmZD8
ag18l7DTVtunJflgJudgyQa/grkgKBj0LrH0rzO0/D4YsCcOJDIbaqSedGBs
vf+uEPetc6wVeGjm4zyGI1YAgez75PRTGVpnCiYZVg8ll/O0fZKXCZHv2Klc
PObJy13V0u8/+5Nos31diC2nraDqd9HGAF5R57KEhO4ze0BfoE6aWnbcLhFz
YxvhayuR+YCn9uMM0W2OEtKxiBszjcwDrb5zvVgU+iROzJh1azFeVc0dFG8E
lyHEkU9wyG55pmMeRZrwrdFwlFcDueGm1XDchKT4q2LC0Ll4+RI8IqrC8uHz
RhE69ELYExNZYXWH76ruWyjsimqWP6NF+fgMIdT5+wPfIpIF5jBBK8cT5542
Kut1oekAc4CwMJeBe634YiyHRHoznAfLH9OMjbCW/F4aTk/bf6NmQtw5kLKM
Yne67SBKjd9m
=8cG/
-----END PGP PUBLIC KEY BLOCK-----
```

We will respond as quickly as possible, usually within 24 hours. To help us fix the issue faster, please send us verifiable proof the vulnerability exists (reproduction steps, screenshot, scripts, videos).

Reward

In appreciation for the effort made:

We will add you to our list of CONTRIBUTORS.

We will send you stickers and t-shirts!

And a huge thank you!