master Disclosures / CVE-2020-14031-Arbitary File Delete-Ozeki SMS Gateway /

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

..

Deletion Start.png	2 years ago
Memory Spike.png	2 years ago
README.md	2 years ago
Result.png	2 years ago
Web View.png	2 years ago

README.md

CVE-2020-14031: Ozeki SMS Gateway Arbitrary File Delete in the "TXT" Module

In Ozeki SMS Gateway software, versions 4.17.6 and below, the “outbox” functionality of the TXT module can be used to delete all/most files in a folder.
Because Ozeki runs as "NT Authority\System" the only files that will not be deleted will be files that are currently being run by the system and/or files that have specific "security attributes" (Ex. Windows Defender files).

This delete functionality can be used to remove important files from different, the most notable of which are:

Folder	Impact
"C:\Windows\"	And subfolders Can be used to delete important system resources, EXEs, DLLs, config files, etc. that may result in an OS level Denial of Service.
The "Ozeki" folder	Can be used to delete: - user config files which will result in users not being able to login when Ozeki restarts - deletion of DLL necessary for Ozeki to start or run services/modules
User files	Can be used to delete user important files such as "Desktop", "Documents", etc. which may result a decrease in productivity, the loss of sensitive personal and/or business materials.

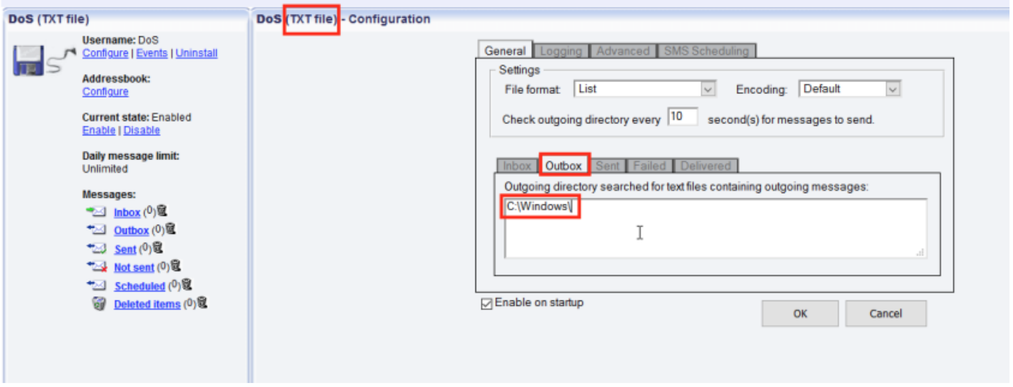
Requirements:

This vulnerability requires:

- Access to an Ozeki Web Application administration interface with rights to create/modify the "outbox" location of a "TXT" Module

Proof Of Concept:

First, we point the TXT "outbox" to a folder from which we want to delete files (Ex. "C:\Windows"):



Username: DoS

Addressbook:

Current state: Enabled

Daily message limit: Unlimited

File format: List

Encoding: Default

Check outgoing directory every 10 second(s) for messages to send.

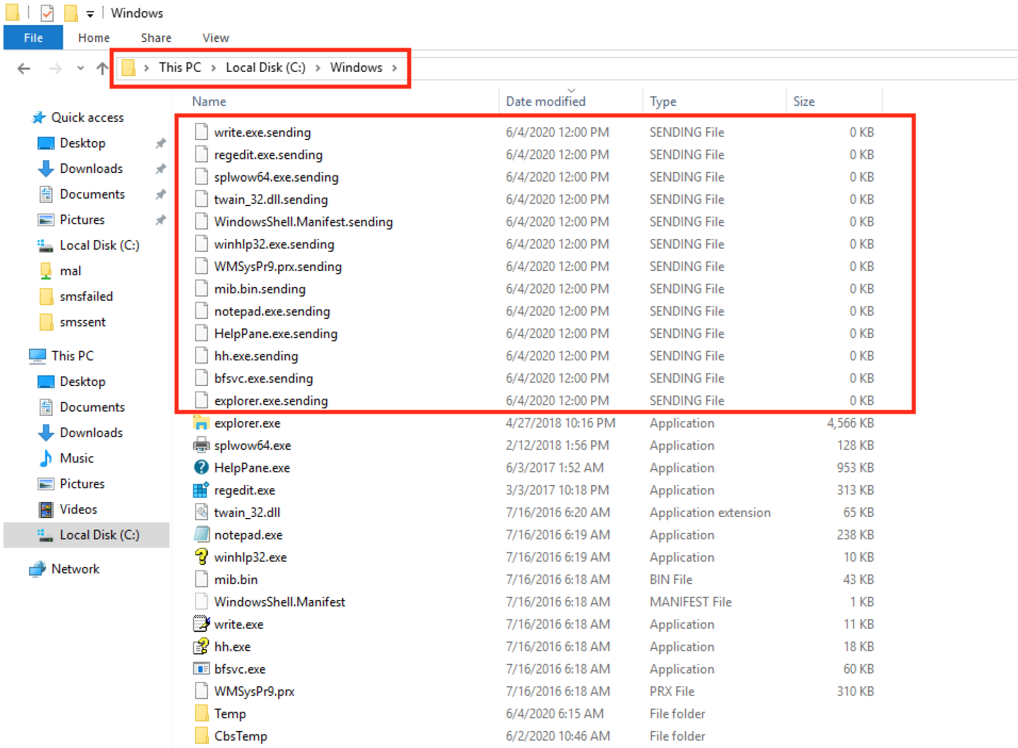
Outgoing directory searched for text files containing outgoing messages:

C:\Windows\

☑ Enable on startup

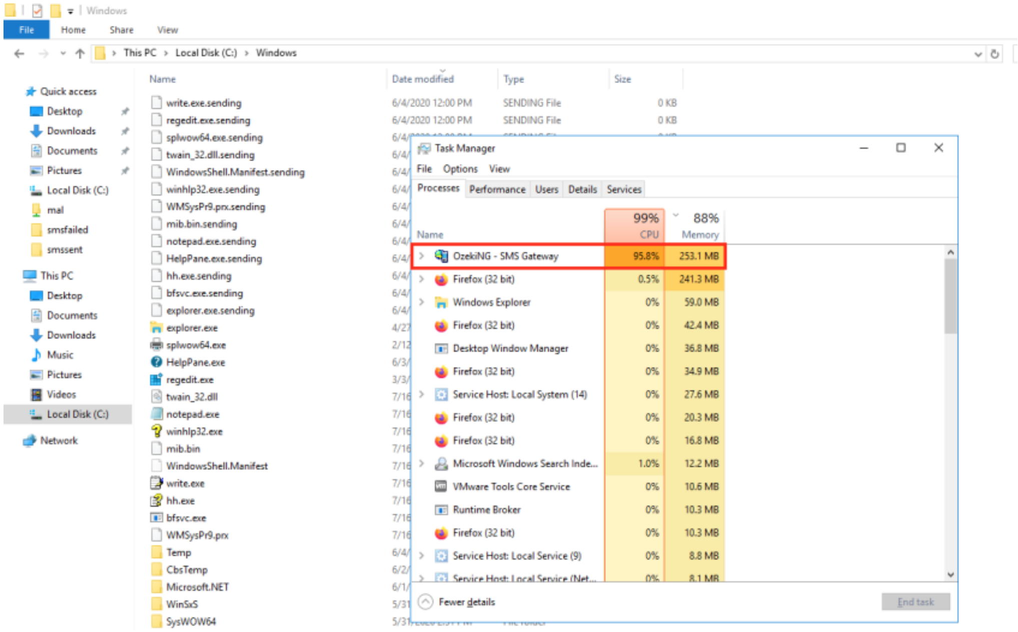
We can notice 2 things almost immediately as this happens:

- Unusual ".sending" files appear as files are getting deleted:



Name	Date modified	Type	Size
write.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
regedit.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
splwow64.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
twain_32.dll.sending	6/4/2020 12:00 PM	SENDING File	0 KB
WindowsShell.Manifest.sending	6/4/2020 12:00 PM	SENDING File	0 KB
winhlp32.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
WMSysPr9.prx.sending	6/4/2020 12:00 PM	SENDING File	0 KB
mib.bin.sending	6/4/2020 12:00 PM	SENDING File	0 KB
notepad.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
HelpPane.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
hh.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
bfsvc.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
explorer.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
explorer.exe	4/27/2018 10:16 PM	Application	4,566 KB
splwow64.exe	2/12/2018 1:56 PM	Application	128 KB
HelpPane.exe	6/3/2017 1:52 AM	Application	953 KB
regedit.exe	3/3/2017 10:18 PM	Application	313 KB
twain_32.dll	7/16/2016 6:20 AM	Application extension	65 KB
notepad.exe	7/16/2016 6:19 AM	Application	238 KB
winhlp32.exe	7/16/2016 6:19 AM	Application	10 KB
mib.bin	7/16/2016 6:18 AM	BIN File	43 KB
WindowsShell.Manifest	7/16/2016 6:18 AM	MANIFEST File	1 KB
write.exe	7/16/2016 6:18 AM	Application	11 KB
hh.exe	7/16/2016 6:18 AM	Application	18 KB
bfsvc.exe	7/16/2016 6:18 AM	Application	60 KB
WMSysPr9.prx	7/16/2016 6:18 AM	PRX File	310 KB
Temp	6/4/2020 6:15 AM	File folder	
CbsTemp	6/2/2020 10:46 AM	File folder	

- A spike in resource consumption and memory happens on the victim:

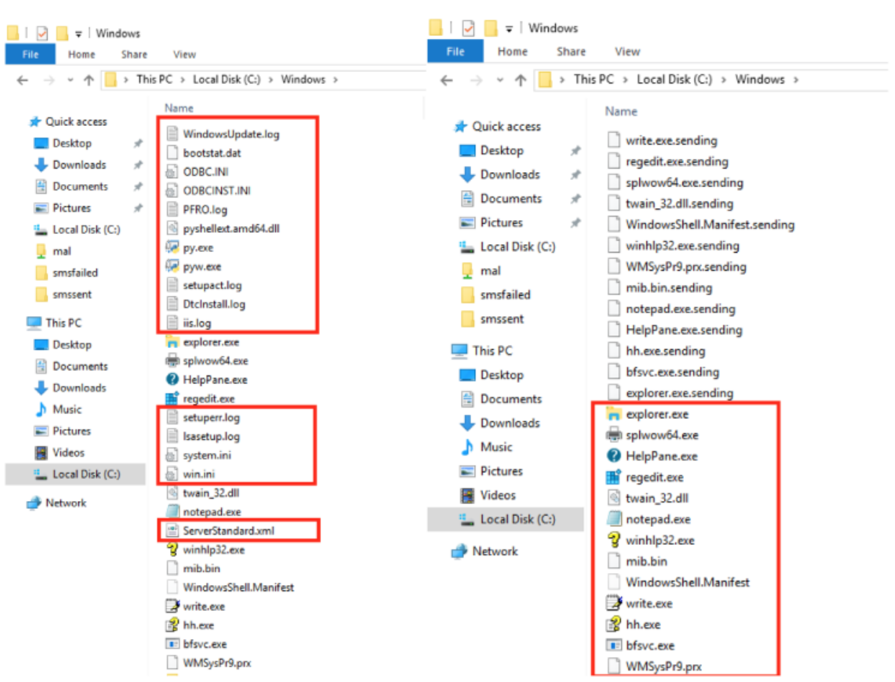


Name	Date modified	Type	Size
write.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
regedit.exe.sending	6/4/2020 12:00 PM	SENDING File	0 KB
splwow64.exe.sending	6/4/		
twain_32.dll.sending	6/4/		
WindowsShell.Manifest.sending	6/4/		
winhlp32.exe.sending	6/4/		
WMSysPr9.prx.sending	6/4/		
mib.bin.sending	6/4/		
notepad.exe.sending	6/4/		
HelpPane.exe.sending	6/4/		
hh.exe.sending	6/4/		
bfsvc.exe.sending	6/4/		
explorer.exe.sending	6/4/		
explorer.exe	4/27		
splwow64.exe	2/12		
HelpPane.exe	6/3/		
regedit.exe	3/3/		
twain_32.dll	7/16		
notepad.exe	7/16		
winhlp32.exe	7/16		
mib.bin	7/16		
WindowsShell.Manifest	7/16		
write.exe	7/16		
hh.exe	7/16		
bfsvc.exe	7/16		
WMSysPr9.prx	7/16		
Temp	6/4/		
CbsTemp	6/2/		
Microsoft.NET	6/1/		
WinSxS	5/31		
SysWOW64	5/31		

Name	99% CPU	88% Memory
OzekiNG - SMS Gateway	95.8%	253.1 MB
Firefox (32 bit)	0.5%	241.3 MB
Windows Explorer	0%	59.0 MB
Firefox (32 bit)	0%	42.4 MB
Desktop Window Manager	0%	36.8 MB
Firefox (32 bit)	0%	34.9 MB
Service Host: Local System (14)	0%	27.6 MB
Firefox (32 bit)	0%	20.3 MB
Firefox (32 bit)	0%	16.8 MB
Microsoft Windows Search Inde...	1.0%	12.2 MB
VMware Tools Core Service	0%	10.6 MB
Runtime Broker	0%	10.3 MB
Firefox (32 bit)	0%	10.3 MB
Service Host: Local Service (9)	0%	8.8 MB
Service Host: Local Service (Net...	0%	8.1 MB

By comparing the "Before" and "After" files, we can see the damage that has been done. In this case:

- Executables and DLLs that were not active at runtime ("py.exe", "pyshellext.amd64.dll", etc.) have been deleted.
- Logfiles ("WindowsUpdate.log", "iis.log", etc.) have been deleted.
- Configuration files ("win.ini", "system.ini", "ServerStandard.xml", etc.) have been deleted.



```
WindowsUpdate.log
bootstat.dat
ODBC.INI
ODBCINST.INI
PFRO.log
pyshellext.amd64.dll
py.exe
pyw.exe
setupact.log
DtcInstall.log
iis.log
explorer.exe
splwow64.exe
HelpPane.exe
regedit.exe
setuperr.log
lsasetup.log
system.ini
win.ini
twain_32.dll
notepad.exe
ServerStandard.xml
winhlp32.exe
mib.bin
WindowsShell.Manifest
write.exe
hh.exe
bfsvc.exe
WMSysPr9.prx
```

```
write.exe.sending
regedit.exe.sending
splwow64.exe.sending
twain_32.dll.sending
WindowsShell.Manifest.sending
winhlp32.exe.sending
WMSysPr9.prx.sending
mib.bin.sending
notepad.exe.sending
HelpPane.exe.sending
hh.exe.sending
bfsvc.exe.sending
explorer.exe.sending
explorer.exe
splwow64.exe
HelpPane.exe
regedit.exe
twain_32.dll
notepad.exe
winhlp32.exe
mib.bin
WindowsShell.Manifest
write.exe
hh.exe
bfsvc.exe
WMSysPr9.prx
```