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

..

README.md	2 years ago
Script Setup.png	2 years ago
View Source.png	2 years ago

README.md

CVE-2020-14021: Ozeki SMS Gateway Arbitrary File Read in the "ASP.net SMS" Module

In the Ozeki SMS Gateway software, versions 4.17.6 and below, the "ASP.net SMS" module can be used to read and validate source code of "ASP" files.
By altering the path to point to an existing file, this functionality can be used to read the file's content with "NT Authority\SYSTEM" privileges.

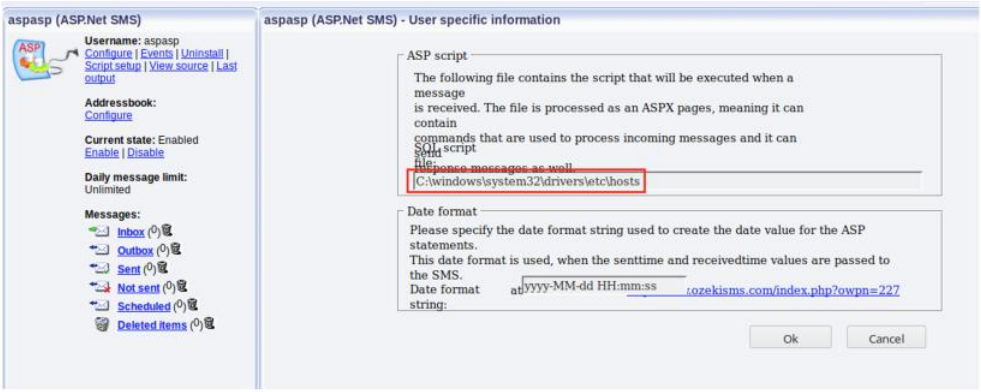
Requirements:

This vulnerability requires:

- Access to an Ozeki Web Application administration interface with rights to create/modify "ASP.Net SMS" script location

Proof Of Concept:

By pointing the "ASP.Net" script to the location of an existing file on the target OS, an attacker can use the "View Source" functionality to then read the content of that file.
In this case we will point the script path to "C:\windows\system32\drivers\etc\hosts".



And now, by using the "View Source" functionality, we can get the contents of the file.