Regular Expression Denial of Service [ReDos]

Regular Expression : A sequence of characters which defines the search pattern is called regular expression. It is generally used to match a string.
Understanding Regular expression :

Symbol	Usage
*	matches zero or more occurrences of the regular expression
+	matches one or more occurrences of the one character regular expression
{..}	repeat the preceding character (or set of characters) for as many times as the value inside this bracket
(?)	tells the computer that the preceding character may or may not be present in the string to be matched
(.)	take place of any other symbol, that is why it is called the wildcard character.
^	tells the computer that the match must start at the beginning of the string or line.

Regex for Email Validation : /^w+[+.w-]*@([w-]+.)*w+[w-]*.([a-z]{2,4}|d+)$/i
The above regex validates the email in following format : abc.edg@gmail.com

How attackers exploits this : If there is weak implementation of RegEx, It is quite possible to perform DoS Attack. Attacker makes the expression to evaluate the value which will make application relatively slow.

Attack Surface: JS Files. Attackers check JS files and see how RegEx are working and wether the application is vulnerable or not

Example : Let’s say a application is accepting user input i.e Color Code which is validated using Regex. Now Attacker/Malicious User can enter malicious payload and make CPU usage rate more thus resulting in DoS.

Resource : https://github.com/2bdenny/ReScue
This tool will identify which RegEx is Vulnerable to ReDoS. It will also list out possible strings for RegEx which can lead to DoS.