1. What is ReDOS (Regular Expression Denial of Service) and what part do ‘Evil Regex’ play?

ReDOS is a situation in which parsing a string via a regular expression causes a major decrease in system processing time due to increasingly consumer resources. Some regular expression patterns are very greedy, thus, ‘evil’, however the way they work is by checking each next possible state. As the length/size of the input increases in combination with the greedy regex, this creates an exponential number of paths required to be checked (Weidman, n.d.).

2. What are the common problems associated with the use of regex? How can these be mitigated?

Certain tokens/special characters in regex are greedy, such as the + (match 1 to unlimited previous characters) and * (match 0 to all previous characters) tokens. Additionally, with the use of brackets to create matching groups, ‘evil’ regexes can be created, for example, (g+)+. The + sign within the bracket allows g to occur as many times, however the same condition gets repeated on the group where the + already persists, creating a repetition.

These can be mitigated by:

1. limiting the number of characters that are permitted to be matched
2. avoiding the use of repetition of special tokens
3. use atomic grouping (Goyvaerts, 2024)

3. How and why could regex be used as part of a security solution?

Regexes can be used in security as part of:

1. logging – quickly and efficiently match unusual patterns or strings

2. firewall – regular expressions can be used to create firewall rules for specific e-mails and network traffic
3. input validation

References:

Goyvaerts, J. (2024) Runaway Regular Expressions: Catastrophic Backtracking. Regular-Expressions.info. Available from: https://www.regular-expressions.info/catastrophic.html [Accessed 14 November 2024]

Li, V. (2020) Regular Expressions: A Quick Intro for Security Professionals. Dzone. Available from: https://dzone.com/articles/regular-expressions-a-quick-intro-for-security-pro [Accessed 14 November 2024]

Weidman, A. (n.d.) Regular expression Denial of Service – ReDoS. OWASP. Available from: https://owasp.org/www-community/attacks/Regular_expression_Denial_of_Service_-_ReDoS [Accessed 14 November 2024]