SQL Slammer

Yasmine Corel

0001010101010101011100011000110001101010
10101VORMWORMWORMWORMWORMWORMWORMWORMWORMWORMW
0010001010010100010100000101010110101010
1010010100010000010101010110101011100011000110011010
0001000001010101010101011100011000110011010
1000110101001110001100011001101010000111011100100100101
01001110001100011001101010100100111011100100100101
100011000110011010000011101110010010010
0110011010100001110111001001001010001010
1010100001110111001001001010001000011010
100111011100100100101000100001101010001000101
01110010010010100010000110101010001000101
001001010001001001101010100010001010010
1010001000011010100010001010010100010000
0000110101010101010101010101010101010101

Vulnerable Software/Language

- Microsoft's SQL Server
- Desktop Engine database products

Vulnerability

SQL Server could allow:

- Access / Modify data
- Compromise SQL servers & server hosts

Exploit

• Must know a valid user name

Timeline



3

Sources

- Symantec Corp. (n.d.). Microsoft SQL Server Resolution Service buffer overflows allow arbitrary code execution. Retrieved February 28, 2019, from http://securityresponse.symantec.com/avcenter/security/Content/2270.html
- Knowles, D. (n.d.). W32.SQLExp.Worm. Retrieved February 28, 2019, from https://www.symantec.com/security-center/writeup/2003-012502-3306-99
- Revolvy, LLC. (n.d.). "SQL Slammer" on Revolvy.com. Retrieved March 1, 2019, from https://www.revolvy.com/page/SQL-Slammer