

Command Injection



This page has been made public for vendors

ABSTRACT

Executing commands from an untrusted source or in an untrusted environment can allow malicious commands to be executed on behalf of an attacker.

EXPLANATION

Command injection vulnerabilities can take the form where an attacker can change the command that the program executes, if the attacker can control what the command is. By executing the command, the application gives an attacker a privilege or capability that the attacker would not otherwise have.

Example 1: The following code reads one line from stdin or whatever device is the current input object, assigns it to the variable listed, and then executes the string.

```
read a
xecute a
```

REFERENCES

1. Standards Mapping - Common Weakness Enumeration - (CWE) *CWE ID 77, CWE ID 78*
2. K. O'Cane. *The MUMPS Programming Language*