# CWE Detail – CWE-506

## Description

The product contains code that appears to be malicious in nature.

## Extended Description

Malicious flaws have acquired colorful names, including Trojan horse, trapdoor, timebomb, and logic-bomb. A developer might insert malicious code with the intent to subvert the security of a product or its host system at some time in the future. It generally refers to a program that performs a useful service but exploits rights of the program's user in a way the user does not intend.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2022-30877: A command history tool was shipped with a code-execution backdoor inserted by a malicious party.

## Related Attack Patterns (CAPEC)

* CAPEC-442
* CAPEC-448
* CAPEC-636

## Attack TTPs

**•** T1027.009: Embedded Payloads (Tactics: defense-evasion)

**•** T1195.001: Compromise Software Dependencies and Development Tools (Tactics: initial-access)

**•** T1218.001: Compiled HTML File (Tactics: defense-evasion)

**•** T1195.002: Compromise Software Supply Chain (Tactics: initial-access)

**•** T1027.003: Steganography (Tactics: defense-evasion)

**•** T1027.004: Compile After Delivery (Tactics: defense-evasion)

**•** T1221: Template Injection (Tactics: defense-evasion)

**•** T1001.002: Steganography (Tactics: command-and-control)

## Modes of Introduction

**•** Implementation: N/A

**•** Bundling: N/A

**•** Distribution: N/A

**•** Installation: N/A

## Common Consequences

**•** Impact: Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Testing: Remove the malicious code and start an effort to ensure that no more malicious code exists. This may require a detailed review of all code, as it is possible to hide a serious attack in only one or two lines of code. These lines may be located almost anywhere in an application and may have been intentionally obfuscated by the attacker. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A

## Notes

**•** Terminology: The term "Trojan horse" was introduced by Dan Edwards and recorded by James Anderson [18] to characterize a particular computer security threat; it has been redefined many times [4,18-20].