VULNERABILITY REPORT

PROJECT NAME:	**sample.c**
REPORT DATE:	**30 Jan, 2024**

[redacted]

[redacted] **BASE_SCORE: 7.4**

Metric	Value
AttackVector	Network
AttackComplexity	High
PrivilegesRequired	None
UserInteraction	Required
Confidentiality	High
Integrity	Low
Availability	Low
Scope	Changed

FIXES

Replace strcpy with strncpy, specifying a maximum length to copy.

SUMMARY
None

[redacted] **BASE_SCORE: 7.5**

Metric	Value
AttackVector	Adjacent
AttackComplexity	Low
PrivilegesRequired	None
UserInteraction	None
Confidentiality	High
Integrity	Low
Availability	Low
Scope	Unchanged

FIXES

Replace `vulnerable_function(input)` with `safe_function(input, 20)`, where `safe_function` performs input validation and truncation before passing the data to the vulnerable function.

SUMMARY

None

[redacted]

[redacted] **BASE_SCORE: 8.1**

Metric	Value
AttackVector	Network
AttackComplexity	High
PrivilegesRequired	None
UserInteraction	None
Confidentiality	High
Integrity	Low
Availability	Low
Scope	Changed

FIXES

Use strncpy() with a fixed size buffer to ensure it doesn't exceed the allocated memory.

SUMMARY

None

[redacted] **BASE_SCORE: 4.2**

Metric	Value
AttackVector	Unknown
AttackComplexity	Low
PrivilegesRequired	None
UserInteraction	None
Confidentiality	None
Integrity	Low
Availability	High
Scope	Unchanged

FIXES

Use `int32_add` function from the C standard library to perform the addition operation, which handles integer overflow correctly.

SUMMARY
None

[redacted] **BASE_SCORE: 7.2**

Metric	Value
AttackVector	Local
AttackComplexity	Low
PrivilegesRequired	None
UserInteraction	None
Confidentiality	Low
Integrity	Low
Availability	High
Scope	Unchanged

FIXES

Replace `strcpy` with `strncpy`, ensuring the destination buffer size is sufficient to accommodate the copied string.

SUMMARY
None

[redacted]

[redacted] **BASE_SCORE: 7.6**

Metric	Value
AttackVector	Local
AttackComplexity	High
PrivilegesRequired	None
UserInteraction	Required
Confidentiality	High
Integrity	Low
Availability	High
Scope	Changed

FIXES

Use `strncpy` function to limit the length of copied data to prevent buffer overflow.

SUMMARY
None

BASE_SCORE: 5.5

Metric	Value
AttackVector	Unknown
AttackComplexity	High
PrivilegesRequired	None
UserInteraction	Required
Confidentiality	High
Integrity	Low
Availability	High
Scope	Unchanged

FIXES

Replace `printf(user_input)` with a safe function like `snprintf()`, ensuring that the input is properly sanitized and escaped to prevent code injection attacks.

SUMMARY
None