

В системе мониторинга сетевого трафика, используемой в организации для обеспечения безопасности корпоративной сети, была обнаружена уязвимость. Система мониторинга отвечает за анализ трафика в реальном времени и идентификацию подозрительных действий, таких как попытки вторжения или аномальное поведение. Уязвимость заключается в недостаточной проверке входных данных, что позволяет злоумышленнику отправлять специально сформированные пакеты, вызывающие переполнение буфера и потенциальное выполнение произвольного кода.

Система мониторинга доступна только из внутренней сети и не имеет прямого доступа из интернета, однако эксплуатация уязвимости может привести к обходу сетевых защитных механизмов и дальнейшему распространению атаки внутри корпоративной сети. Базы данных, связанные с системой мониторинга, содержат метаданные о сетевом трафике и не включают конфиденциальную информацию.

CVSS v4.0 Base Metrics:

Metric	Value	Comments
Attack Vector (AV):	Network (N)	Хоть система мониторинга доступна только из внутренней сети, однако она анализирует трафик, в том числе и из сети интернета. Это означает, что злоумышленник, находясь вне локальной сети может сформировать такой сетевой пакет, который сможет использовать эту уязвимость
Attack Complexity (AC):	Low (L)	Злоумышленник может использовать уязвимость без особых доп.условий (т.е. в любой момент времени)
Attack Requirements (AT):	None (N)	Атака не зависит от специфических условий исполнения
Privileges Required (PR):	None (N)	Злоумышленнику не нужны какие-либо привилегии для использования данной уязвимости
User Interaction (UI):	None (N)	Для атаки злоумышленнику не нужно взаимодействие с другим каким-либо пользователем
Vulnerable System Confidentiality (VC):	None (N)	Базы данных, связанные с системой мониторинга, не содержат конфиденциальную информацию.
Vulnerable System Integrity (VI):	High (H)	Возможность выполнения произвольного кода позволяет злоумышленнику, например, изменить метаданные (или правила детектирования) сетевого трафика
Vulnerable System Availability (VA):	High (H)	Возможность выполнения произвольного кода позволяет злоумышленнику сделать систему мониторинга недоступной (устроить полный отказ в обслуживании)
Subsequent System Confidentiality (SC):	None (N)	Хотя эксплуатация уязвимости и может привести к обходу сетевых защитных механизмов и дальнейшему распространению атаки внутри корпоративной сети - у нас нет

			информации о том, что через эту атаку злоумышленник сможет получить доступ к другим серверам
Subsequent Integrity (SI):	System	None (N)	Хотя эксплуатация уязвимости и может привести к обходу сетевых защитных механизмов и дальнейшему распространению атаки внутри корпоративной сети - у нас нет информации о том, что через эту атаку злоумышленник сможет получить доступ к другим серверам
Subsequent Availability (SA):	System	None (N)	Хотя эксплуатация уязвимости и может привести к обходу сетевых защитных механизмов и дальнейшему распространению атаки внутри корпоративной сети - у нас нет информации о том, что через эту атаку злоумышленник сможет получить доступ к другим серверам

Используя Common Vulnerability Scoring System Version 4.0 Calculator получаем следующее:

CVSS

Common Vulnerability Scoring System Version 4.0 Calculator

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4.0 Score: 8.8 / High

Base Metrics

Exploitability Metrics

Attack Vector (AV): Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC): Low (L) | High (H)

Attack Requirements (AR): None (N) | Present (P)

Privileges Required (PR): None (N) | Low (L) | High (H)

User Interaction (UI): None (N) | Passive (P) | Active (A)

Vulnerable System Impact Metrics

Confidentiality (VC): High (H) | Low (L) | None (N)

Integrity (VI): High (H) | Low (L) | None (N)

Availability (VA): High (H) | Low (L) | None (N)

Subsequent System Impact Metrics

Confidentiality (SC): High (H) | Low (L) | None (N)

Integrity (SI): High (H) | Low (L) | None (N)

Availability (SA): High (H) | Low (L) | None (N)

Supplemental Metrics

Cofactor (C): Not Defined (N) | Nonexistent (N) | Discreet (D)

Таким образом, у нас получается следующее описание:

- 1) Вектор CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N
- 2) CVSS v4.0 Score: 8.8 / High