

В корпоративной сети крупной финансовой организации была обнаружена уязвимость в системе управления конфигурациями серверов. Система управления конфигурациями используется для автоматизации развертывания и поддержания состояния серверов, включая веб-серверы, базы данных и приложения. Уязвимость позволяет злоумышленнику, имеющему доступ к сети, удаленно модифицировать конфигурационные файлы серверов без аутентификации. Это может привести к изменению поведения серверов, внедрению вредоносного кода или даже полному отказу в обслуживании.

Серверы доступны из интернета через брандмауэр и прокси-сервер, но уязвимость в системе управления конфигурациями может быть эксплуатирована только через внутреннюю сеть. Базы данных содержат конфиденциальную информацию клиентов и финансовые данные.

CVSS v4.0 Base Metrics:

Metric	Value	Comments
Attack Vector (AV):	Adjacent (A)	Возможность атаки ограничена тем, что уязвимость может быть эксплуатирована только через внутреннюю сеть.
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):	Low (L)	Злоумышленник должен иметь доступ к сети, т.е. он должен быть авторизован внутри нее. При этом ему не нужны повышенные права для эксплуатации атаки
User Interaction (UI):	None (N)	Для атаки злоумышленнику не нужно взаимодействие с другим каким-либо пользователем
Vulnerable System Confidentiality (VC):	High (H)	Наличие уязвимости позволяет злоумышленнику выполнить произвольный вредоносный код, что означает, что он может получить доступ к чувствительной информации
Vulnerable System Integrity (VI):	High (H)	Наличие уязвимости позволяет злоумышленнику удаленно модифицировать конфигурационные файлы, а также выполнить произвольный вредоносный код - т.е. он может менять конфигурацию системы
Vulnerable System Availability (VA):	High (H)	Наличие уязвимости позволяет злоумышленнику устроить полный отказ в обслуживании
Subsequent System Confidentiality (SC):	High (H)	Система управления конфигурациями используется для управления развертывания и поддержания состояния других серверов, т.е. злоумышленник может получить доступ к чувствительной информации на других серверах

Subsequent Integrity (SI):	System	High (H)	Система управления конфигурациями используется для управления развертывания и поддержания состояния других серверов, т.е. злоумышленник может изменять данные на других серверах
Subsequent Availability (SA):	System	High (H)	Система управления конфигурациями используется для управления развертывания и поддержания состояния других серверов, т.е. злоумышленник может устроить полный отказ в обслуживании на других серверах.

Используя Common Vulnerability Scoring System Version 4.0 Calculator получаем следующее:

The screenshot shows the CVSS 4.0 Calculator interface. The URL bar displays the calculator path: `first.org/cvss/calculator/4-0#CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H`. The interface includes a sidebar with navigation links, a main header with the CVSS logo and calculator title, and a central area for inputting metrics. The calculated score is displayed as **CVSS v4.0 Score: 9.4 / Critical**. The metrics are organized into sections: Base Metrics (Exploitability and Vulnerable System Impact), Subsequent System Impact Metrics, and Supplemental Metrics. The bottom of the page features a footer with a help link, copyright information, and a 'TLPCLEAR' button.

Base Metrics [?]			
Exploitability Metrics			
Attack Vector (AV):	Network (N)	Adjacent (A)	Local (L)
Attack Complexity (AC):	Low (L)	High (H)	
Attack Requirements (AT):	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 [?]			
Safety (S):	Not Defined (N)	Minimal (M)	Disrupt (D)

Таким образом, у нас получается следующее описание:

- 1) Вектор CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
- 2) CVSS v4.0 Score: 9.4 / Critical