

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200722.1 | 22 июля 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Уязвимость аутентификации в SAP NetWeaver AS JAVA

Идентификатор уязвимости

MITRE: CVE-2020-6287

Идентификатор программной ошибки

CWE-287: Некорректная аутентификация

Описание уязвимости

Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти ограничения безопасности и создать пользователя с правами администратора посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных в компоненте LM Configuration Wizard.

Категория уязвимого продукта

Серверное программное обеспечение

Уязвимое ПО

SAP NetWeaver AS JAVA версий 7.30, 7.31, 7.40, 7.50

Рекомендации по устранению

Обновить программное обеспечение

Дата выявления

14 июля 2020 г.

Дата обновления

16 июля 2020 г.

Оценка критичности уязвимости (CVSSv3.1)

10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки (AV)

Сетевой (N)

Сложность эксплуатации уязвимости (AC)

Низкая (L)

Необходимый уровень привилегий (PR)

Отсутствует (N)

Необходимость взаимодействия с
пользователем (UI)

Отсутствует (N)

Масштаб последствий эксплуатации
уязвимости (S)

Изменяется (C)

Влияние на конфиденциальность (C)

Высокое (H)

Влияние на целостность (I)

Высокое (H)

Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-6287 https://www.tenable.com/blog/cve-2020-6287-critical-vulnerability-in-sap-netweaver-application-server-java-disclosed-recon