НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230111.5 | 11 января 2023 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Scala

Идентификатор уязвимости	MITRE: CVE-2022-36944
Идентификатор программной ошибки	CWE-502: Десериализация недоверенных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных.
Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Scala: 2.13.0 - 2.13.8
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	28 декабря 2022 г.
Дата обновления	28 декабря 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	http://github.com/scala/scala/pull/10118 http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L3WMKPFAMFQE3HJVRQ5KOJUTWG264SXI/ http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6ZOZVWY3X72FZZCCRAKRJYTQOJ6LUD6Z/ http://discuss.lightbend.com/t/impact-of-cve-2022-36944-on-akka-cluster-akka-actor-akka-remote/10007/2 http://github.com/scala/scala-collection-compat/releases/tag/v2.9.0