НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200602.2| 2 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд в VMware Spring Security

Идентификатор уязвимости	MITRE: CVE-2020-5407
Идентификатор программной ошибки	CWE-347: Некорректная проверка криптографической подписи
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнять произвольные команды в целевой системе посредством отправки специально сформированного сетевого пакета с вредоносным SAML-ответом. Уязвимость обусловлена некорректной проверкой криптографической подписи SAML-ответов в компоненте spring-security-saml2-service-provider.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Spring Security до v5.2.4, v5.3.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 мая 2020 г.
Дата обновления	21 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/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)	Низкий (L)
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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-5407 https://tanzu.vmware.com/security/cve-2020-5407