НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200813.7 | 13 августа 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Apache HTTP Server

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Apache HTTP Server: 2.4.20, 2.4.21, 2.4.22, 2.4.23, 2.4.24, 2.4.25, 2.4.26, 2.4.27, 2.4.28, 2.4.29, 2.4.32, 2.4.33, 2.4.34, 2.4.35, 2.4.36, 2.4.37, 2.4.38, 2.4.39, 2.4.40, 2.4.41, 2.4.42, 2.4.43
Дата выявления	8 августа 2020 г.
Дата обновления	8 августа 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-11984	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным определением границ буфера памяти при функционировании модуля od_proxy_uwsgi. CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти	8.1

	Рекомендации по устранению: обновить программное обеспечение.	
MITRE: CVE-2020-11993 CVE-2020-9490	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ обслуживания в целевой системе посредством отправки специально сформированных HTTP/2-запросов. Уязвимость обусловлена некорректной обработкой HTTP/2-запросов. CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных CWE-399: Уязвимости, связанные с управлением ресурсами Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	http://httpd.apache.org/security/vulnerabilities_24.html