

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20190820.1 | 20 августа 2019 г.
Уровень опасности: **КРИТИЧЕСКИЙ**

Удаленное выполнение кода в Webmin

Идентификатор уязвимости	MITRE: CVE-2019-15107
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки вредоносного POST-запроса. Уязвимость обусловлена некорректной проверкой предоставленных данных в файле password_change.cgi.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Webmin до v1.930
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 августа 2019 г.
Дата обновления	19 августа 2019 г.
Оценка критичности уязвимости (CVSSv3)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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 (E)

Функциональная версия (F)

Наличие средств устранения уязвимости (RL)

Официальное решение (O)

Достоверность сведений об уязвимости (RC)

Сведения подтверждены (C)

Ссылки на источники

<https://www.pentest.com.tr/exploits/DEFCON-Webmin-1920-Unauthenticated-Remote-Command-Execution.html>

<https://www.exploit-db.com/exploits/47230>

<https://www.tenable.com/plugins/nessus/127911>

<http://www.webmin.com/changes.html>

