НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200401.2 | 1 апреля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в rsyslog для Red Hat Enterprise Linux

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	rsyslog (Red Hat package) версий 8.24.0-12.el7_4, 8.24.0-34.el7, 8.24.0-38.el7 и 8.24.0-41.el7_7 Red Hat Enterprise Linux for Power, little endian версии 7 Red Hat Enterprise Linux for Power, big endian версии 7 Red Hat Virtualization Manager версии 4.3 Red Hat Virtualization for IBM Power LE версии 4 Red Hat Enterprise Linux for IBM z Systems версии 7 Red Hat Enterprise Linux for Scientific Computing версии 7 Red Hat Enterprise Linux Desktop версии 7 Red Hat Enterprise Linux Workstation версии 7 Red Hat Virtualization версии 4 Red Hat Enterprise Linux Server версии 7
Дата выявления	31 марта 2017 г.
Дата обновления	1 апреля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2019-17041	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного пакета уязвимому приложению. Уязвимость обусловлена некорректной работой синтаксического анализатора сообщений журналов AIX в "contrib / pmcisconames / pmcisconames.c". CVSSv3.0: AV:N/AC:L/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 Рекомендации по устранению: Обновить программное обеспечение.	9.8
MITRE: CVE-2019-17042	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного пакета уязвимому приложению. Уязвимость обусловлена некорректной работой синтаксического анализатора сообщений журналов Cisco "contrib / pmcisconames / pmcisconames.c". CVSS:3.0: AV:N/AC:L/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 Рекомендации по устранению: Обновить программное обеспечение.	9.8
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020032701 https://access.redhat.com/security/cve/CVE-2019-17041 https://access.redhat.com/security/cve/CVE-2019-17042	