НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200810.6 | 10 августа 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Juniper Junos OS

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Junos OS 16.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1.
Дата выявления	8 июля 2020 г.
Дата обновления	8 июля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-1649	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным функционированием компонента PFE. 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 Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2020-1650	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным функционированием компонента MS-PIC. 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-400: Неконтролируемое использование ресурсов (Исчерпание ресурсов) Рекомендации по устранению: обновить программное обеспечение.	7.5
MITRE: CVE-2020-1645	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы и обойти службу DNS-фильтрации посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным функционированием компонента MS-PIC. CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных CWE-362: Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (Состояние гонки) Рекомендации по устранению: обновить программное обеспечение.	8.3
MITRE: CVE-2020-1640 CVE-2020-1644 CVE-2020-1646 CVE-2020-1648	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным функционированием компонента RPD. CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных CWE-159: Некорректная обработка специальных элементов CWE-703: Некорректная проверка или обработка исключительных ситуаций CWE-1173: Некорректное использование фреймворка проверки входных данных Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2020-1647 CVE-2020-1654	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы или выполнить код посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным функционированием службы перенаправления ICAP. 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-120: Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера) CWE-415: Двойное освобождение Рекомендации по устранению: обновить программное обеспечение.	9.8

Ссылки на источники	https://kb.juniper.net/JSA11036 https://kb.juniper.net/JSA11028 https://kb.juniper.net/JSA11037 https://kb.juniper.net/JSA11024 https://kb.juniper.net/JSA11033 https://kb.juniper.net/JSA11035 https://kb.juniper.net/JSA11034 https://kb.juniper.net/JSA11031 https://kb.juniper.net/JSA11032