

ИНФОРМАЦИОННАЯ СПРАВКА

от 16 июня 2025 г.

о результатах мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках

УЯЗВИМОСТИ

Опубликована информация о следующих критических уязвимостях программного обеспечения.

Идентификатор и описание	Возможные меры защиты
<p>BDU:2025-06792 CVE-2025-49091</p> <p>Уязвимость эмулятора терминала Konsole среды рабочего стола KDE связана с реализацией некорректного потока управления при обработке URL-схем telnet://, rlogin:// и ssh://. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код при переходе пользователем по специально сформированной ссылке.</p> <p>Имеется информация о средствах эксплуатации уязвимости в открытом доступе (https://www.opennet.ru/opennews/art.shtml?num=63410).</p> <p>Отсутствует информация об использовании уязвимости в реальных атаках.</p> <p>Имеются сведения об использовании эмулятора терминала Konsole среды рабочего стола KDE (Сообщество свободного программного обеспечения) в составе отечественных сертифицированных средств, широко используемых на объектах КИИ.</p> <p>Экспертная оценка требуемого потенциала нарушителя для эксплуатации уязвимости – базовый повышенный потенциал</p>	<p>Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> <p><u>Уровень опасности:</u> Высокий (8.2)</p> <p>CVSS v3: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:L</p> <p><u>Компенсированные меры:</u></p> <ul style="list-style-type: none">- ограничение возможности пользователей перехода по ссылкам, полученным из недоверенных источников;- использование средств изолированной программной среды для открытия ссылок, полученных из недоверенных источников;- использование антивирусного программного обеспечения для проверки ссылок, полученных из недоверенных источников;- использование систем обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимости. <p><u>Использование рекомендаций:</u> https://kde.org/info/security/advisory-20250609-1.txt</p>
<p>BDU:2025-06793 CVE-2024-43706</p> <p>Уязвимость средства мониторинга Synthetics сервиса визуализации данных Kibana связана с недостатками процедуры авторизации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии путем отправки специально сформированного HTTP-запроса.</p> <p>Отсутствует информация о средствах эксплуатации уязвимости в открытом доступе.</p> <p>Отсутствует информация об использовании уязвимости в реальных атаках.</p> <p>Имеются сведения об использовании сервиса</p>	<p>Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> <p><u>Уровень опасности:</u> Высокий (7.6)</p> <p>CVSS v3: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L</p> <p><u>Компенсированные меры:</u></p> <ul style="list-style-type: none">- отключение средства мониторинга Synthetics путем установления значения «false» для параметра xpack.uptime.enabled в файле kibana.yml;- использование межсетевого экрана уровня приложений (WAF) для фильтрации HTTP-трафика;- ограничение доступа к уязвимому программному

<p>визуализации данных Kibana (США) на 22 объектах КИИ.</p> <p>Экспертная оценка требуемого потенциала нарушителя для эксплуатации уязвимости – средний потенциал</p>	<p>обеспечению, используя схему доступа по «белым спискам»;</p> <ul style="list-style-type: none"> - использование систем обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимостей; - минимизация пользовательских привилегий; - отключение/удаление неиспользуемых учётных записей пользователей. <p><u>Использование рекомендаций:</u> https://discuss.elastic.co/t/kibana-8-12-1-security-update-esa-2024-21/379064</p>
---	--

АТАКИ

1. В результате анализа ВПО получен перечень IP-адресов, используемых проукраинскими группировками в качестве объектов DDoS-атак, а также DNS-, прокси-серверов и серверов управления. Перечень IP-адресов актуален по состоянию на 16 июня 2025 года. Выявлены 612 атакуемый IP-адресов российских организаций, относящихся к телекоммуникационной сфере.

Также получены сведения о 400 IP-адресах (в том числе 13 российских – ООО «Стек Дейта Нетворк» в г. Южки (Ленинградская область), Волгоградский филиал ОАО «ЭР-Телеком Холдинг» в г. Волгоград, Самарский филиал ОАО «ВолгаТелеком» в г. Тольятти, ООО «Коммуникации Тайфон» в г. Москва, ООО «КОМТЕХЦЕНТР» в г. Екатеринбург, ООО «СвязьРесурс-Регион» в г. Краснодар, ООО «Связь-энерго» в г. Кострома, ООО «АВАНТА ТЕЛЕКОМ» в г. Краснодар, Тюменский филиал ОАО «ЭР-Телеком Холдинг» в г. Тюмень, ОАО «ВолгаТелеком» в г. Новотроицк (Оренбургская область), АО «Селектел» в г. Москва, ИП Андреев Андрей Григорьевич в г. Ростов-на-Дону, ПАО «Вымпелком» в г. Москва), используемых в атаках в качестве прокси-серверов. Наибольшее число прокси-серверов из следующих стран: США (106 IP-адресов), Индонезия (60 IP-адресов), Китай (51 IP-адрес).

2. Сообщается о DDoS-атаке на информационные системы хостинг-провайдеров RUSONYX (<https://www.rusonyx.ru/>, ООО «Астра Облако», ИНН 7707301630, г. Москва) и ZENON (<https://zenon.net/>, ООО «Зенон Н.С.П.», ИНН 7729126029, г. Москва, организация ликвидирована).

Информация подтверждена.

На момент времени проверки информации (16.06.2025, 10:24) сайт компании RUSONYX недоступен из сети Интернет (ошибка 502).

На сайте компании ZENON (<https://zenon.net/>) опубликована следующая информация: «17 июня 2024 года завершился процесс реорганизации ООО «Зенон Н.С.П.» - теперь компания стала частью ООО «Русоникс». С 23 июля 2024 г. вступили в силу изменения в реквизитах нашей компании. Мы изменили юридическое наименование, юридический адрес и КПП. Новое наименование общества: Общество с ограниченной ответственностью «Астра Облако», краткое наименование: ООО «Астра Облако».

Официальные комментарии представителей компании не обнаружены.

Ни одна из отслеживаемых хакерских группировок не взяла на себя ответственность за атаку на информационные системы хостинг-провайдера ООО «Астра Облако».

Объекты ООО «Астра Облако» фиксируются в качестве целей DDoS-атак проукраинской хакерской группировки IT ARMY ofUkraine.

Источник информации: <https://t.me/antiddositarmyua/1106>.

УТЕЧКИ ДАННЫХ

Информация об обнаруженных утечках данных не относится к области ответственности ФСТЭК России.