Автор: Кубанских О.В., Лоскин В.А.
13.06.2025 16:30 -

УЯЗВИМОСТИ ПРОТОКОЛОВ УДАЛЁННОГО УПРАВЛЕНИЯ И МЕТОДЫ ИХ ЗАЩИТЫ

Кубанских О.В., к.ф.-м.н., доцент,

Лоскин В.А., магистрант,

БГУ им. ак. И.Г. Петровского, г. Брянск, Россия

Аннотация. В статье рассмотрены некоторые уязвимости сетевых протоколов удалённого управления на примере SSH, RDP, VNC и Telnet. Рассмотрены такие уязвимости, как BlueKeep, CVE 2019 17662 и др.Приведены рекомендации, позволяющие снизить риски атак с использованием описанных эксплойтов.

Ключевые слова: SSH, RDP, Telnet, VNC, удалённое администрирование, уязвимости, атаки

В современных информационных системах широкое распространение получили сетевые

протоколы удалённого управления, предназначенные для дистанционного контроляаппаратных средстви программного обеспечения.К числу таких протоколов относятся как устаревший Telnet и его современный и безопасный аналог SSH, предоставляющие доступ к командной строке, так ипротоколы предоставляющие доступ к полноценной графической среде управления удалённого устройства, такие как
RDP
и
VNC
. Эти технологии позволяют существенно повысить эффективность выполнения таких задач, как администрирование и техническая поддержка пользователей, одновременно с этим предоставляя удалённый доступ к вычислительным мощностям корпоративной инфраструктуры.

При всех свои достоинствах, средства удалённого управления могут стать уязвимым звеном в системе безопасности, особенно в случае использования уязвимых версий ПО или ошибки в их конфигурации. Это может стать причиной утечки конфиденциальной информации и другим серьёзным инцидентам.Именно поэтому безопасность протоколов удалённого управления должна рассматриваться как приоритетная задача. Недостаточно просто использовать современные решения – важно постоянно отслеживать новые уязвимости, анализировать их и принимать меры ещё до того, как они будут использованы злоумышленниками.

Одной из наиболее распространённых и опасных угроз, связанных с уязвимыми или неправильно настроенными средствами удалённого управления, являются атаки типа «ManintheMiddle», также известные как MitM-атаки.Их суть заключается в том, что злоумышленник перехватывает сетевой трафик между клиентом и сервером, получая возможность просматривать или модифицировать передаваемые данные [5].

Наибольшему риску таких атак подвержены нешифруемые протоколы, такие какTelnet иVNC, по умолчанию также не шифрующий сеанс удалённого рабочегостола [6].Протокол RDP поддерживает шифрование и проверку подлинности на уровне сети (NLA), однако при использовании самоподписанных сертификатов или отключении проверок возможны атаки с посредником, подменяющим сервер. Даже SSH спроектированый для защищённого соединения уязвим к MitM-атаке в случае, если пользователь проигнорирует предупреждение о смене ключа сервера.

Для эффективной защиты от атак типа «ManintheMiddle» необходимо использовать протоколы, обеспечивающие надёжное шифрование передаваемых данных. В частности, следует отдавать предпочтение SSH,а не Telnet,для протокола VNC — включать шифрование с использованием VPN или SSH-туннеля. Также критически важно осуществлять проверку подлинности сертификатов и ключей, используя доверенные центры сертификации.

Однако использование средствобеспечивающих шифрование передаваемых данных не позволит избежать всех уязвимостей, так как сами реализации протоколов могут содержать ошибки, приводящие к уязвимостям.

Примером этого является уязвимость BlueKeep (CVE-2019-0708) в службе удалённых рабочих столов Microsoft RDP. Эта критическая ошибка была обнаружена в 2019 году и затрагивала не обновлённые версии Windows (от Windows 2000 до Windows 7 и Server 2008 R2). Уязвимость позволяла удалённо выполнить код на целевой системе без

аутентификации. Опасность BlueKeep усугублялась тем, что эксплойт работает на этапе пре-аутентификации и не требует действий со стороны пользователя – таким образом, вредоносное ПО могло автоматически распространяться с одной уязвимой машины на другую[1].

Другой примером могут стать многочисленные уязвимости в реализациях протокола VNC. В 2019 году исследователи Лаборатории Касперского проверили популярные open-source VNC-системы (LibVNC, UltraVNC, TightVNC и др.) и обнаружили 37 уязвимостей, в том числе и CVE 2019 17662, CVE 2019 15692 и многие другие, некоторые из которых существовали десятилетиями. Эксплуатация ряда этих уязвимостей позволяла удалённо выполнить произвольный код на сервере или клиенте VNC [2,4]. Хотя для успешной атаки требовалась хотя бы одноразовая аутентификация, наличие такого количества уязвимостей свидетельствует о серьёзных рисках при использовании VNC без своевременного обновления.

Для защиты от таких уязвимостей, необходимо регулярно обновлять программное обеспечение и следить за рекомендациями разработчиков. Производители систем удалённого доступа оперативно публикуют информацию о найденных уязвимостях в их продукте, а также предлагают меры по их устранению или снижению рисков.

Даже безопасный протокол может быть скомпрометирован при неправильно выполненной настройке. Типичные ошибки конфигурации включают использование устаревших или небезопасных опций, слабых параметров шифрования, а также оставление «по умолчанию» учетных данных. Telnet-серверы часто поставлялись с универсальными паролями по умолчанию. Если администратор не сменил такой пароль,

устройство становится лёгкой добычей для злоумышленника. Массовый пример – устройства интернета вещей, многие из них имеют Telnet-доступ с заводским логином/паролем.

В результате возникла угроза масштабных ботнетов. Так, в 2016 году появился Mirai – вредоносный червь, сканировавший в интернете подключённые по Telnet устройства и использовавший встроенный список из 61 пары логин-пароль для перебора учетных данных администратора. На пике ботнет насчитывал около 400000 заражённых IoT-устройств и использовался для осуществления беспрецедентных по мощности DDoS-атак (до 1 Тбит/с) [3].

Для минимизации рисков, рекомендуется придерживаться принципа безопасной конфигурации по умолчанию. Все неиспользуемые службы (например, Telnet) должны быть отключены. Их наличие в системе создаёт потенциальные векторы атаки, особенно в случае, если доступ открыт во внешние сети.Особое внимание должно быть уделено включению встроенных механизмов безопасности, доступных в современных реализациях протоколов, для RDP – NLA и проверку сертификатов, для VNC – устанавливать сложный пароль доступа и по возможности использовать шифрование. Также необходимо проводить регулярный аудита конфигурации систем и учётных записей.

Таким образом, обеспечение безопасности сетевых протоколов удалённого управления требует комплексного подхода, включающего как технические, так и организационные меры. Их реализация позволяет существенно снизить вероятность успешных атак, направленных на компрометацию систем дистанционного доступа. Необходимо

регулярно отслеживать появление новых уязвимостей (в том числе регистрируемых под идентификаторами CVE), анализировать рекомендации производителей программного обеспечения и проводить аудит текущих конфигураций.

Только системный и проактивный подход к управлению безопасностью удалённого администрирования способен обеспечить надёжную защиту корпоративной информации и устойчивость инфраструктуры в условиях растущих киберугроз.

Литература

1. CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability // National Vulnerability Database. – 2019. – URL: https://nvd.nist.gov/vuln/detail/CVE-2019-0708 (датаобращения: 03.06.2025).

2. Антипов А. В популярных VNC обнаружены многолетние уязвимости // SecurityLab. – 2019. – URL: https://www.securitylab.ru/news/502585.php (дата обращения: 06.06.2025).

3. БотнетMirai: угроза интернету вещей // Хабр. – 2016. – URL: https://habr.com/ru/companies/pt/articles/311754/ (дата обращения: 07.06.2025).

4. Вертинский А. Исследование показало уязвимости в VNC: что делать пользователям // Kaspersky Daily. – 2020. – URL: https://www.kaspersky.ru/blog/vnc-vulnerabilities/25759/ (дата обращения: 03.06.2025).

5. Исследование уязвимостей в VNC [Электронный ресурс] / Kaspersky ICS CERT.–URL: https://ics cert.kaspersky.ru/publications/reports/2019 /11/13/vnc vulnerability research/ (дата обращения: 07.06.2025)

6. Хакеры могут атаковать через устаревшие роутеры Zyxel // Connect-wit.ru. – 2023. – URL: https://www.connect-wit.ru/hakery-mogut-atakovat-cherez-ustarevshie-routery-zyxel.html (дата обращения: 01.06.2025).