Ростелеком
Солар

Отчет
Итоги контроля уязвимостей российских компаний за 2021 год

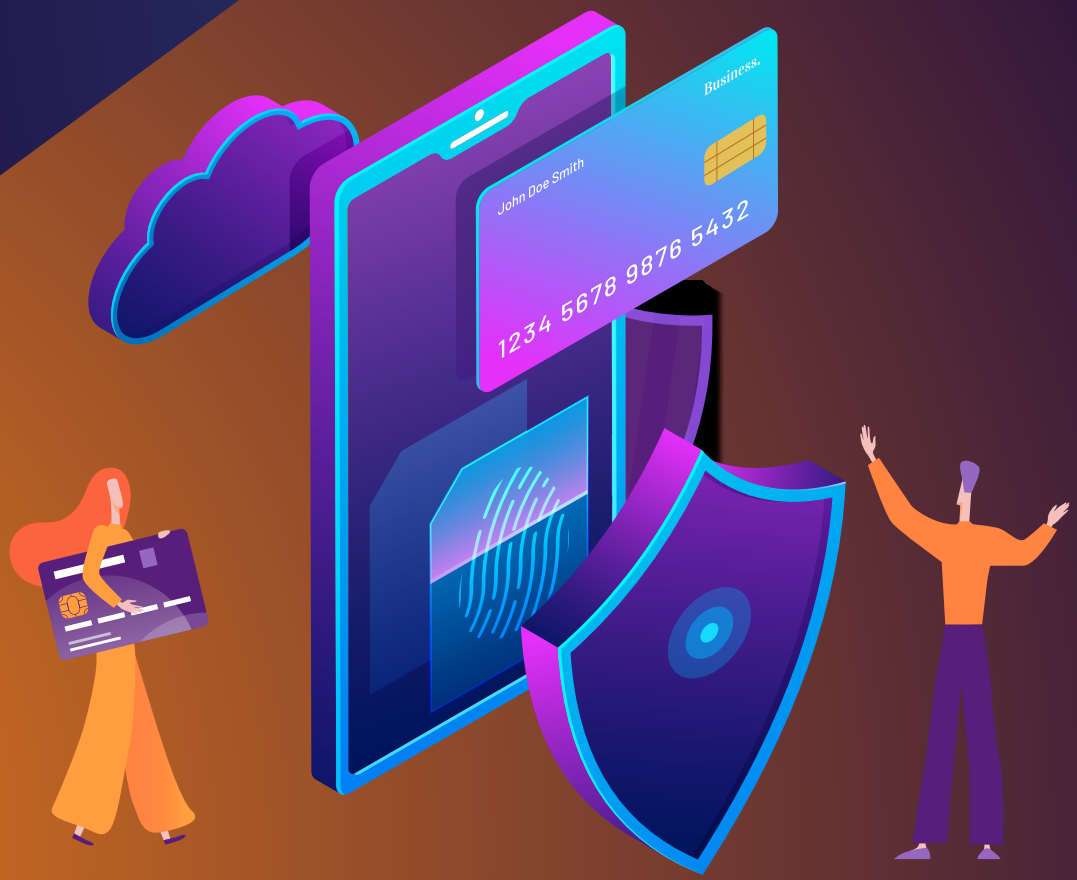
rt-solar.ru

ОГЛАВЛЕНИЕ

Введение

За последние годы ИТ-инфраструктуры многих компаний сильно усложнились, а на периметрах появились новые цифровые активы, закрытые системы и критические серверы, хранящие конфиденциальные данные. Соразмерно с этим растет число уязвимостей разной степени критичности, которыми активно пользуются киберпреступники. Их атаки с использованием найденных ошибок могут привести к финансовым и репутационным потерям, приостановке деятельности компании и даже штрафам со стороны регуляторов. Поэтому первый шаг в построении кибербезопасности организации – это выстраивание процесса по контролю уязвимостей (Vulnerability Management, VM).

В данном отчете собрана статистика уязвимостей, найденных в результате работ по контролю уязвимостей, которые специалисты «Ростелеком-Солар» проводили с помощью сервиса Vulnerability Management (VM) в 2021 году. Всего были проанализированы инфраструктуры более 50 организаций из различных отраслей (ИТ, промышленность, ритейл, медицина, госструктуры).



Методология

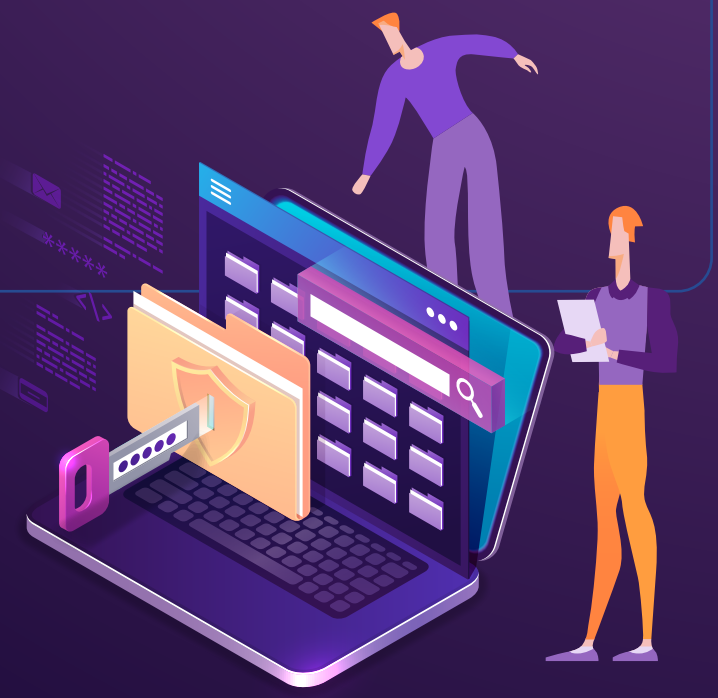
В рамках выполнения работ специалисты «Ростелеком-Солар» проводили инструментальное сканирование в режимах **Blackbox** и **Whitebox.**

Blackbox – сканирование без использования учетных записей и авторизации. В этом случае сканер может обнаружить уязвимости только в доступных ему сетевых сервисах, проверив текущую защищенность хоста на основании баннеров, ответов на специально сконфигурированные запросы и т. п. Как правило, **Blackbox чаще используют при сканировании внешнего периметра.**

Whitebox – сканирование с использованием учетных записей и авторизации. В этом случае сканер проверяет не только внешние интерфейсы, но и получает авторизованный доступ к установленному ПО, реестру и т. д. Это существенно расширяет область проверки и позволяет выявить наличие необходимых обновлений и актуальных уязвимостей (например, ошибки в конфигурации сервисов или возможности нелегитимного повышения привилегий). **Такой метод чаще используется для сканирования внутреннего периметра.**

При анализе результатов сканирования учитывалась локализация уязвимостей, найденных:

- на внешнем сетевом периметре;
- на внутреннем сетевом периметре;
- в веб-приложениях.



Ключевые выводы

Все исследуемые компании использовали небезопасные методы шифрования или испытывали трудности с сертификатами или конфигурацией, способные нарушить целостность данных и привести к их перехвату злоумышленниками. Данная проблема может быть устранена выполнением корректных настроек.

Для **75%** обнаруженных уязвимостей существуют способы исправления (патчи, руководство по устранению и т. п.). Остальные уязвимости представляют собой end-of-life программы, проблемы с шифрованием и сертификатами, использование устаревших протоколов, некоторые типы RCE и прочие уязвимости, которые невозможно закрыть патчем. В этих случаях требуются новые настройки или замена ПО и сертификатов.

В компаниях часто не устанавливаются обновления ПО и ОС, что указывает на проблемы с патч-менеджментом. Данная проблема ведет к увеличению привлекательности ИТ-ресурсов компаний для злоумышленников и большим финансовым и репутационным потерям в случае кражи данных.

Большая часть **(94%)** уникальных уязвимостей имеют уровень критичности выше среднего. При этом многие критические ошибки имеют опубликованный эксплойт, что значительно упрощает жизнь злоумышленника.

Часто встречаются уязвимости старше 20 лет, в среднем же окно возможностей злоумышленника составляет 10–12 лет (разница между наиболее старой и наиболее новой уязвимостью с эксплойтом, обнаруженной в инфраструктуре).

Общая статистика по проведенным работам

Всего в рамках проведения работ было выявлено 153 336 уязвимостей (в том числе повторяющихся), из них 7558 (то есть 5%) – уникальные.

Большая часть (94%) уникальных уязвимостей имеет уровень критичности выше среднего. Еще 5% – средний уровень, 1% – минимальный. Данная статистика указывает на то, что у инфраструктур компаний достаточно низкий уровень защищенности и они являются привлекательными для злоумышленников.

Для 75% найденных уязвимостей существуют способы устранения (патчи, руководство по устранению/исправлению и т. п.), но при этом они все еще не закрыты. Данная статистика говорит о том, что в большинстве компаний либо очень слабый патч-менеджмент, либо его вообще нет. Это также подтверждается и огромным количеством неустановленных обновлений безопасности: 45% уязвимостей можно закрыть патчами.

Остальные 25% уязвимостей представляют собой end-of-life программы, проблемы с шифрованием и сертификатами, использование устаревших протоколов, некоторые типы RCE и прочие уязвимости, которые невозможно закрыть патчем. В этом случае требуются новые настройки или замена ПО/сертификатов.

Топ-5 проблем сетевого периметра

65% уязвимости, связанные с отсутствующими обновлениями безопасности ПО (security updates);

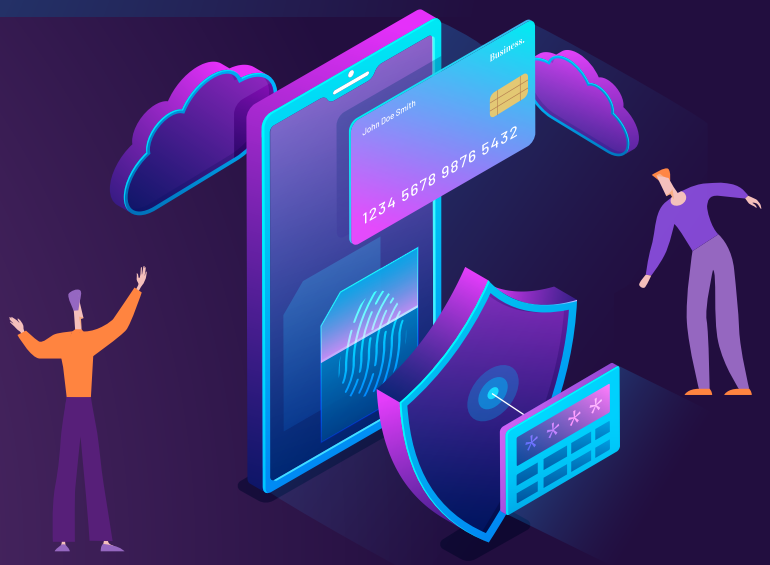
14% уязвимости, связанные с шифрованием передаваемых данных и используемыми протоколами (SSL/TLS);

7% уязвимости, позволяющие злоумышленнику выполнять произвольный код (code execution);

6% уязвимости, связанные с используемыми SSL-сертификатами (SSL certificate);

6% уязвимости, приводящие к долговременному отказу оборудования (DOS);

2% остальное.



Сканирование внутреннего сетевого периметра

В ходе работ по сканированию внутреннего сетевого периметра было обнаружено 147 133 уязвимости. Из них уникальных – 7527 (5 %). Большая часть (95%) уникальных уязвимостей имеет уровень критичности выше среднего. Еще 5% – средний уровень, 1% – минимальный.

Для **79%** найденных недостатков существуют способы устранения (патч, руководства по устранению/исправлению и т. п.).

Наиболее часто встречающиеся уязвимости во внутреннем сегменте связаны с:

- шифрованием;
- обновлениями безопасности ПО;
- парольным и пользовательским учетом.

Из трендовых уязвимостей, о которых много говорили в ИБ-сообществе и в СМИ, в инфраструктурах до сих пор встречаются **Log4j, BlueKeep, ShellShock, PrintNightmare, ProxyShell, EternalBlue.**

Сканирование внешнего сетевого периметра

В ходе работ по сканированию внешнего сетевого периметра было обнаружено 1478 уязвимостей, из которых 262 – уникальные, то есть 18%. Большая часть (82%) уникальных уязвимостей имеют уровень критичности выше среднего.
Еще 20% – средний уровень, 8% – минимальный.

Для **73%** обнаруженных уязвимостей существуют способы устранения (патчи, руководство по устранению/исправлению и т. п.).

Наиболее часто во внешнем сегменте встречаются уязвимости, связанные с:

- шифрованием;
- настройкой и обновлением веб-серверов.

Следует отметить, что трендовых уязвимостей на внешних периметрах компаний обнаружено не было, однако мы регулярно фиксируем проблемы с их инвентаризацией (компании не знают весь свой пул внешних адресов) и критическое количество уязвимостей, связанных с неправильной настройкой или полным отсутствием шифрования данных.

Сканирование веб-приложений

В ходе работ по сканированию веб-приложений было обнаружено 4893 уязвимости. Из них 38 – уникальные, то есть менее 1%.
Большая часть (55%) уникальных уязвимостей имеют уровень критичности выше среднего. Еще 24% – средний уровень, 21% – минимальный.

Топ-5 проблем в веб-приложениях

56%	использование уязвимых и устаревших компонентов;
23%	возможность использования инъекций и проведения атак типа «межсайтовый скриптинг (XSS)»;
8%	проблемы шифрования;
5%	использование уязвимых конфигураций безопасности;
4%	использование уязвимых конфигураций безопасности;
4%	остальное.

Ростелеком
Солар

rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70