Key words: *small-scale specialized equipment, municipal specialized equipment, construction specialized equipment, gardening equipment, production processes, economic benefits.*

Сведения об авторах

Азамат Сабиржанович Жакупов – главный инженер компании «JAS Engineering»; e-mail: erkosh911@gmail.com.

Еркен Болатович Алжанов* – EMBA Менеджмент, Project Manager IPMA C, миноритарный партнер и Project Manager компании «JAS Engineering»; e-mail: erkosh911@gmail.com.

Авторлар туралы

Азамат Сабыржанович Жакупов – «JAS Engineering» компаниясының негізін қалаушы және бас инженері; e-mail: erkosh911@gmail.com.

Еркен Болатұлы Алжанов* – EMBA Менеджмент, Project Manager IPMA C, «JAS Engineering» компаниясының миноритарлық серіктесі және Project Manager; e-mail: erkosh911@gmail.com.

Author Information

Azamat Sabirzhanovich Zhakupov – Founder and Chief Engineer of «JAS Engineering»; e-mail: erkosh911@gmail.com.

Erken Bolatovich Alzhanov* – EMBA in Management, Project Manager IPMA C, minority partner and Project Manager of «JAS Engineering»; e-mail: erkosh911@gmail.com.

Поступила в редакцию 02.10.2024
Поступила после доработки 18.11.2024
Принята к публикации 19.11.2024

https://doi.org/10.53360/2788-7995-2024-4(16)-14

МРНТИ: 81.93.29

И.Х. Ташенов, А.К. Шайханова*
Евразийский национальный университет имени Л.Н. Гумилева,
050000, Республика Казахстан, г.Астана, ул.Пушкина, 11
*e-mail: shaikhanova_ak@enu.kz

АНАЛИЗ УЯЗВИМОСТИ ERP-СИСТЕМ SAP: ИССЛЕДОВАНИЕ ПРОБЛЕМЫ RECON И ЕЁ ВЛИЯНИЯ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Аннотация: *Киберугрозы становятся всё более изощрёнными, представляя значительный риск для корпоративных систем управления ресурсами (ERP), таких как SAP, которые обеспечивают критически важные процессы крупных организаций. Одной из самых серьёзных уязвимостей в SAP является RECON (CVE-2020-6287), получившая максимальную оценку 10 по шкале CVSSv3. Такая высокая оценка указывает на критическую опасность уязвимости, позволяющей злоумышленникам, не имеющим авторизации, получить административный доступ к системам. Это может привести к утечкам конфиденциальных данных, дестабилизации бизнес-процессов и компрометации финансовой информации.*

Для решения проблемы RECON в статье рассматриваются три ключевых инструмента. INSTANT RECON от Onapsis обеспечивает быстрое выявление уязвимости, минимизируя временной лаг между её обнаружением и устранением. Offline Security предлагает методы защиты от угроз, применяемые в изолированных системах. SAP Enterprise Threat Detection (ETD) позволяет мониторить активность в реальном времени, предотвращая потенциальные атаки. Эти инструменты играют важнейшую роль в защите данных и обеспечении стабильности бизнес-процессов. Их использование помогает повысить устойчивость ERP-систем перед внутренними и внешними угрозами, укрепляя общую информационную безопасность организаций.

Ключевые слова: *системы управления ресурсами, бизнес-процессы, контроль доступа, безопасность данных, безопасность приложений, уязвимость, INSTANT RECON, Offline Security, аналитика.*

Введение. С каждым годом киберугрозы становятся все более сложными и разнообразными, представляя серьезную опасность для корпоративных информационных систем. Особенно это касается систем управления предприятием (ERP), таких как SAP, которые являются сердцем операционной деятельности многих крупных организаций по всему миру. SAP, будучи одной из самых популярных и сложных ERP-систем, регулярно оказывается в центре внимания злоумышленников, стремящихся найти уязвимости, которые позволят им получить доступ к критически важной информации и бизнес-процессам.

Одной из наиболее значимых и опасных уязвимостей, обнаруженных в SAP в последние годы, стала уязвимость RECON (CVE-2020-6287). Она получила наивысший балл по шкале критичности CVSSv3 – 10 из 10, что подчеркивает ее серьезность. RECON позволяет неаутентифицированным злоумышленникам получить полный административный доступ к системам SAP, что может привести к утечке конфиденциальных данных, изменению бизнес-процессов, компрометации финансовых данных и другим критическим последствиям. Эта уязвимость присутствует в компонентах SAP NetWeaver и затрагивает множество модулей, таких как SAP S/4HANA, SAP CRM, SAP SCM и другие.

Безопасность ERP-систем становится ключевым фактором успешной работы любой компании, ведь они обеспечивают управление основными ресурсами, финансовыми потоками и производственными процессами. В условиях постоянного повышения уровня угроз информационной безопасности организациям крайне важно иметь эффективные инструменты для выявления и предотвращения эксплуатации уязвимостей.

В данной статье рассмотрим три инструмента, которые могут помочь в выявлении и устранении уязвимости RECON в SAP-системах: INSTANT RECON от компании Onapsis, Offline Security, а также специализированное решение SAP для обнаружения угроз в реальном времени – SAP Enterprise Threat Detection (ETD). Эти инструменты играют важную роль в комплексной стратегии защиты SAP-систем от внешних и внутренних угроз, обеспечивая надежность и целостность корпоративных данных и бизнес-процессов.

Условия и методы исследования. В исследовании проанализированы концепции обеспечения безопасности в среде SAP, которые включают три основных аспекта: контроль доступа, безопасность данных и безопасность приложений. Для поддержания высокого уровня защиты SAP-системы необходимо реализовать строгие меры по каждому из этих направлений. Например, обязательным условием является применение многофакторной аутентификации (MFA) для управления доступом, особенно для внешних пользователей. Политика безопасности данных должна строго регламентировать доступ к информации по ролям, а управление привилегированным доступом (PAM) призвано защищать систему от несанкционированного вмешательства.

Методы исследования включают анализ уязвимости RECON в компоненте SAP NetWeaver, которая позволяет злоумышленникам получать административный доступ к системе. Для выявления и устранения этой уязвимости применялись три инструмента:

- INSTANT RECON от Onapsis – инструмент, обеспечивающий быстрое выявление уязвимости RECON, который позволяет администраторам SAP оперативно сканировать системы и получать детализированные отчеты для принятия мер.
- Offline Security – клиент-серверное приложение для анонимного анализа безопасности SAP-систем, позволяющее выявить уязвимости без компрометации данных компании. Отчет включает детализированную информацию о критичности угроз и рекомендации по их устранению.
- SAP Enterprise Threat Detection (ETD) – инструмент, разработанный SAP для постоянного мониторинга и выявления угроз в режиме реального времени. Он использует корреляцию событий и моделей угроз для обнаружения подозрительных действий, позволяя предотвращать возможные атаки до нанесения ущерба.

Эти методы исследования были выбраны в связи с необходимостью комплексного подхода к защите SAP-систем от внешних и внутренних угроз, и направлены на обеспечение целостности и безопасности корпоративных данных и процессов.

Результаты исследований

Концепции безопасности SAP. Безопасность SAP охватывает три основные области кибербезопасности: контроль доступа, безопасность данных и безопасность приложений. Для

обеспечения безопасности среда SAP подлежит строгому контролю доступа, а системные данные должны быть максимально защищены. Наконец, само приложение должно быть защищено строгими гарантиями безопасности. На практике согласованная работа всех трех концепций безопасности SAP означает применение лучших доступных инструментов и методов обеспечения безопасности в среде SAP. Например, если организация использует многофакторную аутентификацию (MFA) для предоставления разрешения на доступ к сети внешним мобильным пользователям, этот контроль также должен применяться ко всем остальным, желающим получить доступ к системам SAP. Затем в SAP политика безопасности данных должна обеспечивать соблюдение ограничений доступа к данным по ролям. Защита приложения включает в себя управление исправлениями и строгий контроль управления привилегированным доступом (PAM), чтобы гарантировать, что ни один посторонний человек не сможет получить административный доступ к серверной части SAP. Также нужно упомянуть о социальной инженерии. Ведь социальная инженерия в контексте SAP представляет серьезную угрозу безопасности, поскольку злоумышленники могут использовать манипуляции и обман для получения конфиденциальной информации или выполнения вредоносных действий в системе SAP. Атаки фишингом, маскировкой под официальные уведомления и манипуляции персоналом могут привести к раскрытию учетных данных, несанкционированным доступам и изменениям данных. Обман сотрудников поддержки и убеждение в обновлении или установке вредоносного ПО также могут быть результатом социальной инженерии, создавая уязвимости в безопасности SAP и подрывая целостность системы. Поэтому эффективные меры обучения сотрудников и внедрение строгих политик безопасности являются неотъемлемыми частями обеспечения безопасности в среде SAP [1, 2].

Внедрение SAP-систем в предприятиях приносит множество выгод, таких как повышение эффективности и улучшение управления ресурсами. Однако, в силу своей сложности и широкого спектра функциональности, SAP также становится объектом интереса для киберпреступников, которые могут стремиться получить несанкционированный доступ к конфиденциальной информации, нарушить бизнес-процессы или провести атаки с целью вымогательства. Существуют различные виды и типы атак на SAP системы, такие как: инъекции кода, перехват данных, атаки на доступность и т.д. В данной статье, я хотел бы рассмотреть уязвимость системы, воспользовавшись которой, злоумышленники атаковали SAP системы по всему миру. На данный момент инженеры SAP уже исправили опасную ошибку CVE-2020-6287. уязвимости дали название RECON (аббревиатура от Remotely Exploitable Code On NetWeaver) и она получила 10 баллов из 10 по шкале оценки уязвимостей CVSSv3. Такой рейтинг означает, что ошибка крайне проста в использовании, и ее эксплуатация почти не требует технических знаний. Также уязвимость может быть использована для автоматизированных удаленных атак и не требует, чтобы злоумышленник уже имел учетную запись в приложении SAP или знал чужие учетные данные [3, 4].

Если не аутентифицированный злоумышленник сможет подключиться к службе HTTP(S) и успешно воспользоваться уязвимостью RECON, в некоторых ситуациях последствия могут быть критическими. Технически говоря, злоумышленник сможет создать нового пользователя в уязвимой системе SAP с максимальными привилегиями (роль администратора), минуя все средства контроля доступа и авторизации (такие как разделение обязанностей, управление идентификацией и решения GRC). Это означает, что злоумышленник может получить полный контроль над затронутой системой SAP, ее базовыми бизнес-данными и процессами. Наличие административного доступа к системе позволит злоумышленнику управлять (читать/изменять/удалять) каждой записью базы данных или файлом в системе. Из-за неограниченного доступа, который злоумышленник может получить, воспользовавшись неисправленными системами, эта уязвимость может представлять собой недостаток в ИТ-контролях предприятия в соответствии с нормативными требованиями, что потенциально влияет на соответствие финансовым требованиям (SarbanesOxley) и конфиденциальности (GDPR) [5, 6].

Использование уязвимости позволяет злоумышленнику выполнить ряд вредоносных действий, в том числе:

- Кража личной информации (PII) у сотрудников, клиентов и поставщиков
- Чтение, изменение или удаление финансовых записей

- Изменение банковских реквизитов (номер счета, номер IBAN и т. д.)
- Администрирование процессов закупок
- Нарушить работу системы, повредив данные или полностью выключив ее
- Удалить или изменить трассировки, журналы и другие файлы

Данная уязвимость находится в компоненте по умолчанию, который входит в состав всех SAP-приложений, работающих на стеке Java SAP NetWeaver версий 7,30-7,5. Речь о компоненте LM Configuration Wizard, который является частью SAP NetWeaver Application Server (AS). Данный компонент используется во множестве популярных продуктов, включая SAP S/4HANA, SAP SCM, SAP CRM, SAP CRM, SAP Enterprise Portal, а также SAP Solution Manager (SolMan). Другие приложения SAP, работающие со стеком SAP NetWeaver Java, тоже подвержены уязвимости. Специалисты Onapsis предполагают, что число компаний, которые затрагивает данная проблема, равно примерно 40 000, хотя не все они «светят» уязвимыми приложениями в интернете. Так, проведенное исследователями сканирование показало, что в сети можно обнаружить около 2500 SAP-систем, которые в настоящее время уязвимы перед проблемой RECON (33% в Северной Америке, 29% в Европе и 27% в Азиатско-Тихоокеанском регионе) [7, 8].

Обсуждение научных результатов

Как не допустить использование данной уязвимости? Администраторам SAP-систем рекомендуется установить патчи, которые доступны на сайте SAP. А для того, чтобы не допустить данной уязвимости следует использовать сканеры, которые быстро помогают организациям оценить, подвергаются ли их приложения SAP риску, помогают обнаружить подозрительную активность, связанную с эксплуатацией уязвимостей, в том числе и RECON (CVE-2020-6287). Далее будут рассмотрены 3 инструмента, которые могут помочь обнаруживать подобного рода уязвимости.

INSTANT RECON от Onapsis. Компания Onapsis, являющаяся лидером в области безопасности SAP-систем, разработала инструмент INSTANT RECON, который предназначен для быстрого и эффективного выявления уязвимости RECON. Этот инструмент предоставляет администраторам SAP возможность сканировать свои системы на наличие данной уязвимости и моментально получать результаты. INSTANT RECON – это бесплатное решение с открытым исходным кодом, доступное на GitHub, что делает его доступным для широкого круга специалистов по информационной безопасности.

Инструмент сканирует уязвимые компоненты SAP NetWeaver и помогает администраторам оперативно выявить необходимость применения патчей, что существенно снижает риски для бизнеса.

Основным преимуществом INSTANT RECON является его простота использования и оперативность. Администратор может запустить сканирование в течение нескольких минут и получить детализированный отчет, указывающий, какие системы требуют незамедлительных мер. Этот инструмент рекомендуется использовать в первую очередь для тех организаций, чьи SAP-системы имеют внешний доступ через интернет, так как такие системы подвержены наиболее высоким рискам.[9]

Offline Security. Offline Security – это клиент-серверное приложение, которое предназначено для анализа безопасности SAP-систем. Данный инструмент уникален тем, что весь процесс анализа проводится в анонимной форме, что делает его безопасным для организаций, обеспокоенных конфиденциальностью своих данных. Администратор собирает необходимые данные о системе (безопасно маскируя такие параметры, как IP-адреса и имена серверов), после чего отправляет информацию на сервер для анализа.

По завершению анализа пользователь получает подробный отчет с результатами в формате Excel, который включает критичность выявленных уязвимостей и рекомендации по их устранению.

Такой подход позволяет специалистам по безопасности легко сортировать уязвимости по приоритетам и оперативно принимать меры по их устранению. Offline Security отличается высокой степенью детализации отчетов, что делает его незаменимым инструментом для тех, кто хочет глубже изучить состояние безопасности своих SAP-систем и понять, какие шаги необходимы для устранения угроз (рис. 1).

В отчете присутствует функция сортировки, а на первой странице можно увидеть расширенную аналитику по количеству найденных нот и их критичности. Ноты помогают решить проблему и зачастую в них описаны шаги решения проблемы (рис. 2) [10].

Software Component	Version	Support Package	Note ID	Note Title	Description
ST-PI	2008_1_710	SAPKITLREM	2835979	Code Injection	Service Data Download in SAP Application Server ABAP (ST-PI), before versions 2008_1_46C, 2008_1_620, 2008_1_640, 2008_1_700, 2008_1_710, 740 allows an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application and the whole ABAP system leading to Code Injection.
SAP_BW	731	SAPKW73117	2986980	Multiple vulnerabilities	The BW Database Interface allows an attacker with low privileges to execute any crafted database queries, exposing the backend database. An attacker can include their own SQL commands which the database will execute without properly sanitizing the untrusted data leading to SQL injection vulnerability which can fully compromise the affected SAP system.
SAP_BW	731	SAPKW73117	2999854	Code Injection	SAP Business Warehouse, versions 700, 701, 702, 711, 730, 731, 740, 750, 782 and SAP BW/4HANA, versions 100, 200, allow a low privileged attacker to inject code using a remote enabled function module over the network. Via the function module an attacker can create a malicious ABAP report which could be used to get access to sensitive data, to inject malicious UPDATE statements that could also impact the operating system, to disrupt the functionality of the SAP system which can thereby lead to Denial of Service.
SAP_BASIS	731	SAPKB73119	3294595	Directory Traversal	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable.
SAP_BASIS	731	SAPKB73119	3302162	Directory Traversal	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable.
SAP_BASIS	731	SAPKB73119	3097887	Improper Authorization	The software logistics system of SAP NetWeaver AS ABAP and ABAP Platform versions 700, 701, 702, 710, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, enables a malicious user to transfer ABAP code artifacts or content by bypassing the established quality controls.

Рисунок 1 – Отчет в Excel

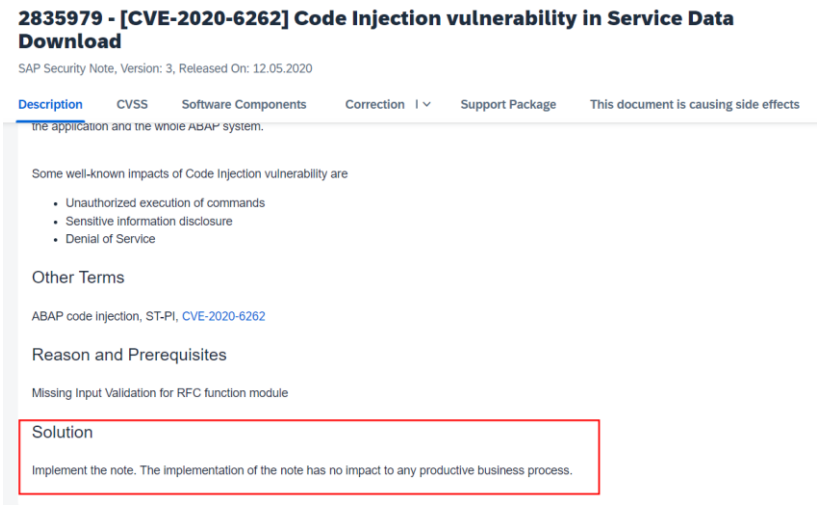

Рисунок 2 – Нота из отчета Excel

SAP Enterprise Threat Detection (ETD). SAP Enterprise Threat Detection (ETD) – это решение, разработанное самой компанией SAP для выявления угроз в режиме реального времени. В отличие от предыдущих инструментов, SAP ETD ориентировано на постоянный мониторинг событий и активности в системе. Оно анализирует поведение пользователей и системы, выявляя аномалии, которые могут свидетельствовать о попытках эксплуатации уязвимостей, таких как RECON [11].

SAP ETD использует метод корреляции событий и моделей угроз, что позволяет своевременно обнаружить подозрительные действия и предотвратить возможные атаки до того, как они нанесут ущерб. Например, если злоумышленник пытается воспользоваться уязвимостью RECON для получения административного доступа, SAP ETD сможет выявить аномальные действия, такие как создание новых пользователей или попытки изменения конфигурации системы, и предупредить администратора о необходимости вмешательства (рис. 3) [12].

Преимущество SAP ETD (рис. 4) заключается в его интеграции с другими продуктами SAP, что позволяет организациям получать комплексную картину безопасности своих систем. Решение поддерживает работу с различными модулями SAP, включая S/4HANA, что делает его универсальным инструментом для обеспечения безопасности в масштабах всего предприятия [13].

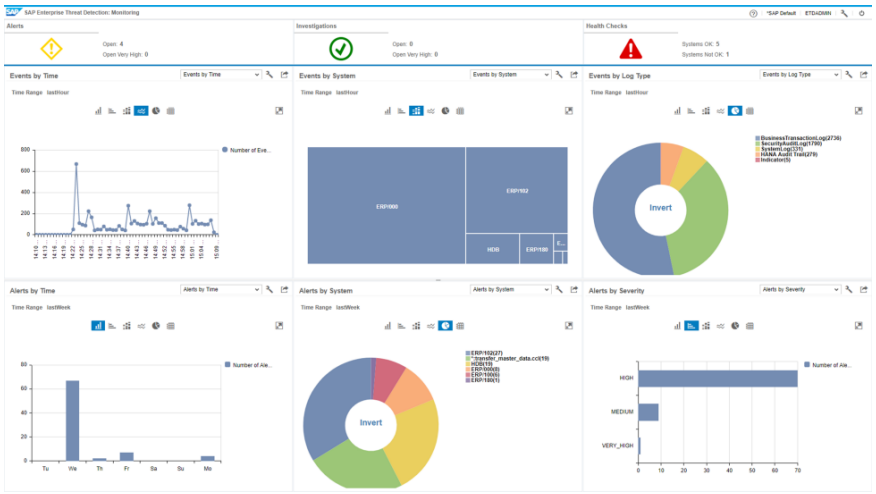

Рисунок 3 – Мониторинг событий SAP ETD

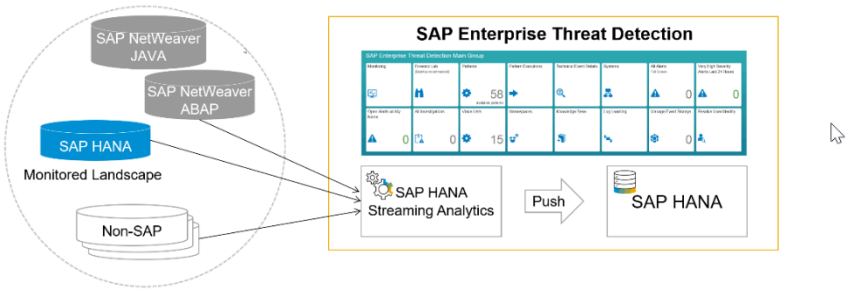

Рисунок 4 – Интеграция со всеми продуктами SAP

Заключение. Уязвимость RECON (CVE-2020-6287) стала серьёзным напоминанием о важности информационной безопасности в системах управления ресурсами предприятия (ERP), таких как SAP. Как центральный элемент для управления бизнес-процессами в крупнейших мировых организациях, SAP-системы представляют собой ключевую мишень для злоумышленников, стремящихся получить доступ к конфиденциальным данным и нарушить операционные процессы. Угроза, которую несет RECON, показала, что даже самые защищенные и проверенные временем системы могут содержать критические уязвимости, эксплуатация которых может привести к серьезным последствиям, включая потерю данных, нарушение бизнес-операций и репутационные риски.

Внедрение современных инструментов для обеспечения безопасности, таких как INSTANT RECON от Onapsis, Offline Security и SAP Enterprise Threat Detection (ETD), предоставляет возможность не только своевременно обнаруживать уязвимости, но и предотвращать их эксплуатацию. Эти инструменты обеспечивают комплексную защиту, начиная от быстрого сканирования системы и получения отчетов об уязвимостях до постоянного мониторинга и анализа подозрительной активности. Благодаря использованию этих решений компании могут существенно сократить риски, связанные с киберугрозами, и создать более надежную защиту для своих бизнес-процессов.

Однако важно понимать, что использование инструментов выявления уязвимостей – это лишь один из шагов на пути к защите корпоративных систем. Безопасность SAP-систем требует многоуровневого подхода, включающего регулярное обновление программного обеспечения, внедрение политик управления доступом, обучение сотрудников и создание надежной инфраструктуры безопасности. Только комплексная и проактивная стратегия безопасности позволит минимизировать риски, обеспечить защиту данных и сохранить целостность бизнес-процессов.

Таким образом, уязвимость RECON стала ярким примером того, как быстро развиваются киберугрозы и насколько важно своевременно реагировать на них. Постоянное совершенствование методов защиты и использование передовых решений безопасности позволит компаниям сохранить устойчивость в условиях постоянных кибератак и обеспечить стабильное развитие в цифровой среде.

Список литературы

1. Davenport T.H. Implementing Enterprise Systems in Enterprises / T.H. Davenport // Harvard Business Review. – 1998. – P. 121-131. https://maaw.info/ArticleSummaries/ ArtSumDavenport98.htm
2. Rein Schmidt J. Securing SAP Applications Using a Secure Software Lifecycle / J. ReinSchmidt, G. François. – 2019. – 256 p.
3. U.S. Department of Commerce. (2018). Enterprise Resource Planning (ERP) Planning Guide. – 189 p.
4. SAP Company Website. URL: https://me.sap.com/notes/2934135 (date of application: 01.09.2024).
5. SAP SE. (2021). SAP ERP Central Component (SAP ECC). URL: https://www.sap.com/central-asia-caucasus/index.html?url_id=auto_hp_redirect_central-asia-caucasus (date of application: 01.09.2024).
6. SAP Security Community. URL: https://pages.community.sap.com/topics/security (date of application: 04.09.2024).
7. Onapsis Research Labs. (2020). RECON: URL: https://onapsis.com/threat-research/recon/ (date of application: 15.09.2024).
8. Common Vulnerabilities and Exposures (CVE). (2020). Details of CVE-2020-6287. URL: https://www.securitylab.ru/news/510313.php (date of application: 27.09.2024).
9. National Vulnerability Database NIST. (2020). NVD – CVE-2020-6287. URL: https://nvd.nist.gov/vuln/detail/CVE-2020-6287 (date of application: 27.09.2024).
10. Offline Security. URL: https://github.com/offlinesec/offlinesec-client (date of application: 28.09.2024).
11. Onapsis. (2021). URL: https://onapsis.com/ (date of application: 01.10.2024).
12. INSTANT RECON. URL: https://github.com/chipik/SAP_RECON/tree/master (date of application: 01.10.2024).
13. SAPinsider. (2021). Complete Guide to SAP Security. URL: https://sapinsider.org/ (date of application: 05.10.2024)

I.K. Tashenov, A.K. Shaikhanova*

L.N. Gumilyov Eurasian National University

050000, Republic of Kazakhstan Astana,Pushkina str., 11

*e-mail: shaikhanova_ak@enu.kz

ANALYSIS OF SAP ERP SYSTEM VULNERABILITIES: INVESTIGATING THE RECON ISSUE AND ITS IMPACT ON INFORMATION SECURITY

Cyber threats are becoming increasingly sophisticated, posing a significant risk to enterprise resource planning (ERP) systems, such as SAP, which support the critical processes of large organizations. One of the most serious vulnerabilities in SAP is RECON (CVE-2020-6287), which received the maximum score of 10 on the CVSSv3 scale. Such a high rating indicates the critical danger of the vulnerability, allowing unauthorized attackers to gain administrative access to the systems. This can lead to data leaks, destabilization of business processes, and compromise of financial information.

To address the RECON issue, the article examines three key tools. INSTANT RECON from Onapsis ensures rapid vulnerability detection, minimizing the time lag between discovery and remediation. Offline Security offers threat protection methods applied in isolated systems. SAP Enterprise Threat Detection (ETD) allows monitoring activity in real-time, preventing potential attacks. These tools play a crucial role in data protection and ensuring the stability of business processes. Their use helps enhance the resilience of ERP systems against internal and external threats, strengthening the overall information security of organizations.

Key words: *resource management systems, business processes, access control, data security, application security, vulnerability, INSTANT RECON, Offline Security, , analytics.*

И.Х.Ташенов, А.К. Шайханова*

Л.Н. Гумилев атындағы Еуразия ұлттық университеті,

050000, Қазақстан Республикасы, Астана қ., Пушкин к-сі, 11

*e-mail: shaikhanova_ak@enu.kz

ERP ЖҮЙЕЛЕРІНДЕГІ ОСАЛДЫҚТАРДЫ ТАЛДАУ: RECON МӘСЕЛЕСІН ЗЕРТТЕУ ЖӘНЕ ОНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ӘСЕРІ

Киберқауіптер барған сайын күрделене түсуде, бұл ірі ұйымдардың маңызды процестерін қамтамасыз ететін SAP сияқты корпоративтік ресурстарды басқару жүйелеріне (ERP) айтарлықтай қауіп төндіреді. SAP-Тегі ең үлкен осалдықтардың бірі-CVSSv3 шкаласы бойынша ең жоғары 10 балл алған RECON (CVE-2020-6287). Мұндай жоғары баға авторизациясы жоқ шабуылдаушыларға жүйелерге әкімшілік қол жеткізуге мүмкіндік беретін осалдықтың маңызды қаупін көрсетеді. Бұл құпия деректердің бұзылуына, бизнес-процестердің тұрақсыздығына және қаржылық ақпараттың бұзылуына әкелуі мүмкін. Recon мәселесін шешу үшін мақалада үш негізгі құрал қарастырылады. Onapsis ' s INSTANT RECON осалдықты тез анықтауға мүмкіндік береді, оны анықтау мен жою арасындағы уақыт артта қалуын азайтады. Offline Security оқшауланған жүйелерде қолданылатын қауіп-қатерден қорғау әдістерін ұсынады. SAP Enterprise Threat Detection (ETD) ықтимал шабуылдардың алдын алу арқылы нақты уақыттағы әрекеттерді бақылауға мүмкіндік береді. Бұл құралдар деректерді қорғауда және бизнес-процестердің тұрақтылығын қамтамасыз етуде маңызды рөл атқарады. Оларды пайдалану ұйымдардың жалпы ақпараттық қауіпсіздігін нығайта отырып, ERP жүйелерінің ішкі және сыртқы қауіптерге қарсы тұрақтылығын арттыруға көмектеседі..

Түйін сөздер: *ресурстарды басқару жүйелері, бизнес-процестер, кіруді басқару, деректер қауіпсіздігі, қолданба қауіпсіздігі, осалдық, INSTANT RECON, Offline Security, аналитика.*

Сведения об авторах

Ильяс Хакимович Ташенов – магистрант кафедры «Информационная безопасность»; Евразийский национальный университет им. Л.Н. Гумилева, Республика Казахстан; e-mail: Ilyas.tashenov@bk.ru. ORCID: https://orcid.org/my-orcid?orcid=0009-0006-6644-1492.

Айгуль Кайрулаевна Шайханова* – PhD, профессор кафедры информационной безопасности, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Республика Казакстан; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Авторлар туралы мәліметтер

Ильяс Хакімұлы Ташенов – «Ақпараттық қауіпсіздік» кафедрасының магистранты; Л.Н. Гумилев атындағы Еуразия ұлттық университеті; Астана, Қазақстан Республикасы; e-mail: Ilyas.tashenov@bk.ru. ORCID: https://orcid.org/my-orcid?orcid=0009-0006-6644-1492.

Айгуль Кайрулақызы Шайханова* – PhD, ақпараттық қауіпсіздік кафедрасының профессоры; Л.Н. Гумилев атындағы Еуразия ұлттық университеті; Астана, Қазақстан Республикасы; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Information about the authors

Ilyas Khakimovich Tashenov – master's degree student of the Department of Information Security; L.N.Gumilyov Eurasian National University, Republic of Kazakhstan; e-mail: Ilyas.tashenov@bk.ru. ORCID: https://orcid.org/my-orcid?orcid=0009-0006-6644-1492.

Aigul Kayrulaevna Shaikhanova* – PhD, Professor of the Department of Information Security, L.N. Gumilyov Eurasian National University; Astana, Republic of Kazakhstan; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Поступила в редакцию 20.11.2024
Поступила после доработки 21.11.2024
Принята к публикации 22.11.2024

https://doi.org/10.53360/2788-7995-2024-4(16)-15

МРНТИ: 28.15.19

А.Е. Найманов, А.К. Шайханова*
Казахский университет технологии и бизнеса имени К. Кулажанова,
Казахстан, г.Астана, ул. Кайыма Мухамедханова, 37А
*e-mail: aigul.shaikhanova@gmail.com

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПРОГРАММНЫХ ИНСТРУМЕНТОВ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ