

Table of Contents

Table of Contents	1
Изменения в UserGate SIEM 7	2
UserGate SIEM 7.4.0(build 7.4.0.175635R, 23/06/2025)	3
UserGate SIEM 7.4.0(build 7.4.0.170259R, 16/06/2025)	5
UserGate SIEM 7.3.1(build 7.3.1.153682R, 12/05/2025)	7
UserGate SIEM 7.3.1(build 7.3.1.149025R, 01/05/2025)	9
UserGate SIEM 7.2.2(build 7.2.2.149026R, 01/05/2025)	10
UserGate SIEM 7.3.0(build 7.3.0.123359R, 19/03/2025)	11
UserGate SIEM 7.3.0(build 7.3.0.116739R, 05/03/2025)	13
UserGate SIEM 7.2.1(build 7.2.1.115866R, 04/03/2025)	15
UserGate SIEM 7.3.0(build 7.3.0.113300R, 26/02/2025)	17
UserGate SIEM 7.2.0(build 7.2.0.76784R, 16/12/2024)	18
UserGate SIEM 7.2.0(build 7.2.0.70211R, 29/11/2024)	20
UserGate SIEM 7.2.0(build 7.2.0.67150R, 21/11/2024)	22
UserGate SIEM 7.2.0(build 7.2.0.60375R, 07/11/2024)	24
UserGate SIEM 7.1.2(build 7.1.2.33025R, 27/08/2024)	26
UserGate SIEM 7.1.2(build 7.1.2.30045R, 20/08/2024)	28
UserGate SIEM 7.1.1(build 7.1.1.12162R, 24/06/2024)	30
UserGate SIEM 7.1.0(build 7.1.0.1704R, 02/04/2024)	32
UserGate Log Analyzer 7.1.0 Release Candidate 2(build 7.1.0.1612RC, 07/02/2024)	35
UserGate SIEM 7.1.0 Release Candidate (build 7.1.0.1605RC, 16/11/2023)	36
UserGate SIEM 7.0.1(hotfix сборка 7.0.1.1052R, 10/06/2024)	38
UserGate SIEM 7.0.1(hotfix сборка 7.0.1.1051R, 08/04/2024)	39
UserGate Log Analyzer 7.0.1 (hotfix сборка 7.0.1.1043R, 13/03/2024)	41
UserGate Log Analyzer 7.0.1 (hotfix сборка 7.0.1.1022R, 4/12/2023)	43
UserGate Log Analyzer 7.0.1 (hotfix сборка 7.0.1.1020R, 24/11/2023) Отозван	45

Version: 7.x
Product: SIEM
Release Notes: 

Статус

Бета

Внимание! Версия в стадии бета-тестирования и не рекомендуется для массовой установки в производственную инфраструктуру (production). Задача этой сборки: проверка в "боевых условиях" у лояльных клиентов, сбор обратной связи и выявление потенциальных недостатков на ранней стадии.

Новые возможности

№ задачи	Описание
SUM-4874	Обновлены стили Web интерфейса.
SUM-13228	Добавлена возможность импорта/экспорта правил нормализации в файл (бинарный формат).
SUM-13270	Добавлена функциональность выбора последовательности срабатывания правил нормализации через Web интерфейс.
SUM-14799	Добавлена фильтрация дублирующихся событий syslog для UserID агента.

Улучшения и оптимизации

№ задачи	Описание
SUM-12943	Оптимизирована скорость обработки событий.
SUM-16503	Оптимизирована работа с сетевыми соединениями при запросах.
SUM-16644	Оптимизирован расход ресурсов CPU.

Исправления

№ задачи	Описание
SUM-15840	Выведена информация в Дашборде о новых типах ограничений в лицензии.
SUM-16380	Исключена возможность занятия порта 9009 системными сервисами.
SUM-17164	Исправлена работа корреляции событий, раздела аналитики в SIEM.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

Не обнаружено.

Контрольные суммы файлов

Имя файла	MD5	Ufix
siem_x86_update_7.4.0.175635R.bin	722e3986e46d52b047f544c3bdcf37c3	F2145A84B5EFC0B0

Имя файла	MD5	Ufix
siem7-x86-hdd.bz2	1706772412ea445dc3bacf852d74cdac	CCF47AB1301EC7F7
siem7-x86-hyperv.zip	4c939a87df6113fb99d248c6f7ce91e6	D125204CD489AF71
siem7-x86-qcow2.zip	db5357a323f2ed9be752203639e5c2af	3BD8B27CA4448F69
siem7-x86-ovf.ova	7642998794d0ad0a3ffcc51415af6d0d	446DFFF495E17AC9

Product: SIEM
Release Notes: ☒

Статус

Отозвано

Внимание! Версия в стадии бета-тестирования и не рекомендуется для массовой установки в производственную инфраструктуру (production). Задача этой сборки: проверка в "боевых условиях" у лояльных клиентов, сбор обратной связи и выявление потенциальных недостатков на ранней стадии.

Новые возможности

№ задачи	Описание
SUM-13228	Добавлена возможность импорта/экспорта правил нормализации в файл (бинарный формат).
SUM-13270	Добавлена функциональность выбора последовательности срабатывания правил нормализации через Web интерфейс.
SUM-14799	Добавлена фильтрация дублирующихся событий syslog для UserID агента.

Улучшения и оптимизации

№ задачи	Описание
SUM-16503	Оптимизирована работа с сетевыми соединениями при запросах.
SUM-16644	Оптимизирован расход ресурсов CPU.

Исправления

№ задачи	Описание
SUM-15840	Выведена информация в Дашборде о новых типах ограничений в лицензии.
SUM-16380	Исключена возможность занятия порта 9009 системными сервисами.
SUM-17164	Исправлена работа корреляции событий, раздела аналитики в SIEM.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

Не обнаружено.

Контрольные суммы файлов

Имя файла	MD5	Ufix
siem_x86_update_7.4.0.170259R.bin	efe958379ca8beb2b0fb6513a56027b6	1A036A51C2CE4515
siem7-x86-hdd.bz2	acb84b5951a0f164a82baac29ef4688d	FAE6D3E6A9BE1CA2
siem7-x86-hyperv.zip	aef5540c1763af9ff6547f9af391fcc6	68E086D791A1A6F6

Имя файла	MD5	Ufix
siem7-x86-qcow2.zip	0fec752db24c0636d4e4c9c54bb57cca	286364097C7BA2DB
siem7-x86-ovf.zip	0fec752db24c0636d4e4c9c54bb57cca	286364097C7BA2DB

Version: 7.3.x
Release Notes: ☒

Статус

Стабильно

Новые возможности

Отсутствуют.

Улучшения и оптимизации

№ задачи	Описание
SUM-16644	Оптимизирован расход ресурсов CPU на платформах с с большим количеством ядер.

Исправления

№ задачи	Описание
SUM-16219	Устранена уязвимость, позволяющая произвести обход директорий (path traversal) устройства NGFW в определенных случаях.
SUM-17023	Исправлена ошибка, приводящая к невозможности установки offline пакета обновлений.
SUM-17063	Устранена уязвимость, позволяющая неавторизованному пользователю исполнить произвольную команду ОС через интерфейс CLI, используя специально сформированный запрос.
SUM-16551	Исправлена уязвимость, позволяющая получить общие сведения о платформе UserGate с использованием специально сформированных запросов.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-16380	Системные сервисы могут занять порт 9009, зарезервированный для соединения между узлами кластера.	В следующих версиях ПО.
SUM-17164	Некорректно работает корреляция событий, раздел аналитика.	В следующих версиях ПО.

Контрольные суммы файлов

Имя файла	MD5	Ufix
siem_x86_update_7.3.1.153682R.bin	98b31211b8afb8e854c5b40ac3d6d31c	A838829D72640F2F
siem7-x86-hdd.bz2	4e5a4f516a3e6bd2ef296c7230e89ed7	C6F7B705A0E89BEB
siem7-x86-hyperv.zip	9384bc751b4ae92f1e3ebdfaad38258b	00612E0668B93B65

Имя файла	MD5	Ufix
siem7-x86-qcow2.zip	26cd95ddfd50c04e47813dbc00fbb3a	543948BD874E59E8
siem7-x86-ovf.zip	5ceac01c3f07c8ea010c100ab8666537	C48FF5328C0508DA

Product: SIEM
Version: 7.3.x
Release Notes: 

Статус

Отозвано

Новые возможности

Отсутствуют.

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-16219	Устранена уязвимость, позволяющая произвести обход директорий (path traversal) устройства NGFW в определенных случаях.
SUM-17023	Исправлена ошибка, приводящая к невозможности установки offline пакета обновлений.
SUM-17063	Устранена уязвимость, позволяющая неавторизованному пользователю исполнить произвольную команду ОС через интерфейс CLI, используя специально сформированный запрос.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

Не обнаружено.

Контрольные суммы файлов

Имя файла	MD5	Ufix
siem_x86_update_7.3.1.149025R.bin	950b277fa543fcc30cec95538debe003	4CD31511A4520C3A
siem7-x86-hdd.bz2	89eb8536b29415cb5a5175a0f88b90e1	0E080F3A5C3F5C87
siem7-x86-hyperv.zip	584b001e8c14db7276140d577bf0b53f	87C20E36BEB0A411
siem7-x86-qcow2.zip	3047ec8f1b538c93fe04375f029ae90c	D49E6BE288CCB27E
siem7-x86-ovf.zip	138750b1db5928fc47f2ff1042bfab98	148E634C32127C72

Version: 7.2.x
Product: SIEM
Release Notes: 

Статус

Стабильно

Новые возможности

Отсутствуют.

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-16219	Устранена уязвимость, позволяющая произвести обход директорий (path traversal) устройства NGFW в определенных случаях.
SUM-16541	Исправлена уязвимость, позволяющая осуществить перехват соединения удаленного помощника.
SUM-17063	Устранена уязвимость, позволяющая неавторизованному пользователю исполнить произвольную команду ОС через интерфейс CLI, используя специально сформированный запрос.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

Не обнаружено.

Контрольные суммы файлов

Имя файла	MD5	Ufix
siem_x86_update_7.2.2.149026R.bin	e0ce54b9ac6556492e023afbfc89601a	14172DA0
siem7-x86-hdd.bz2	e0ce54b9ac6556492e023afbfc89601a	14172DA0
siem7-x86-hyperv.zip	e0ce54b9ac6556492e023afbfc89601a	14172DA0
siem7-x86-qcow2.zip	e0ce54b9ac6556492e023afbfc89601a	14172DA0
siem7-x86-ovf.zip	e0ce54b9ac6556492e023afbfc89601a	14172DA0

Product: SIEM
Release Notes: ☒

Статус

Стабильно

Новые возможности

№ задачи	Описание
SUM-7555	Выпущен SIEM в виде отдельного продукта. Logan и SIEM технически разведены для самостоятельного развития в рамках экосистемы SUMMA. Важно! старые инсталляции SIEM 7.1.x 7.2.x нельзя апдейтить до нового SIEM 7.3.x , необходима новая инсталляция.
SUM-4859	Добавлена возможность создания кластера отказоустойчивости для SIEM (актив-пассив). Добавлен новый тип узла кластера Арбитратор, обеспечивающий консистентность данных.
SUM-12938	Добавлена библиотека экспертизы правил нормализации для различных источников событий от MRC UserGate, позволяющая оперативно и корректно подключить источники событий в инфраструктуре заказчика. Библиотека нормализации доступна в базовой лицензии продукта.
SUM-10186	Добавлена возможность использования списков URL категорий в поисковых запросах в аналитике и поиске.
SUM-10188	Добавлена возможность использования списков приложений в поисковых запросах в аналитике и поиске.

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-9929	Введена новая система лицензирования. Теперь SIEM лицензируется по ядрам (эквивалент 1cpu = 1000 Event Per Second). Без лицензии подключение источников недоступно, с активированной лицензией ограничение снимается.
SUM-11415	Исправлена невозможность удалить сенсор UserGate.
SUM-14275	Исправлена ошибка приводящая к неработоспособности метода аутентификации radius после обновления версии.
SUM-15253	Исправлена уязвимость, позволяющая при наличии административного доступа в web консоль администратора выполнять произвольные команды на уровне ОС.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Внимание!Обновление с предыдущих версий невозможно! Только чистая установка.
Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

Не обнаружено.

Контрольные суммы файлов

Имя файла	MD5	Ufix
siem_x86_update_7.3.0.123359R.bin	a82cf590b8cafc1cf1c831b773cba4cf	42CFEE98E844AF1A

Имя файла	MD5	Ufix
siem7-x86-hdd.bz2	9beb1f70c1e7e55d9ebe73f3831b1e6a	F350462A0A29DC60
siem7-x86-hyperv.zip	872e2554872ed932a0dc6248f162e8f3	2F903B8DAC21F949
siem7-x86-qcow2.zip	e6c70484810933850367902c747947bc	2AE3D6D0D2DA3E53
siem7-x86-ovf.zip	2762623b35fc680639531cbdde5fdbea	917E285AE93F596D

Release Notes: ☒
Product: SIEM
Version: 7.3.x

Статус

Бета

Внимание! Версия в стадии бета-тестирования и не рекомендуется для массовой установки в производственную инфраструктуру (production). Задача этой сборки: проверка в "боевых условиях" у лояльных клиентов, сбор обратной связи и выявление потенциальных недостатков на ранней стадии.

Новые возможности

№ задачи	Описание
SUM-7555	Выпущен SIEM в виде отдельного продукта. Logan и SIEM технически разведены для самостоятельного развития в рамках экосистемы SUMMA. Важно! старые инсталляции SIEM 7.1.x 7.2.x нельзя апдейтить до нового SIEM 7.3.x , необходима новая инсталляция.
SUM-4859	Добавлена возможность создания кластера отказоустойчивости для SIEM (актив-пассив). Добавлен новый тип узла кластера Арбитратор, обеспечивающий консистентность данных.
SUM-12938	Добавлена библиотека экспертизы правил нормализации для различных источников событий от MRC UserGate, позволяющая оперативно и корректно подключить источники событий в инфраструктуре заказчика. Библиотека нормализации доступна в базовой лицензии продукта.

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-9929	Введена новая система лицензирования. Теперь SIEM лицензируется по ядрам (эквивалент 1cpu = 1000 Event Per Second). Без лицензии подключение источников недоступно, с активированной лицензией ограничение снимается.
SUM-14275	Исправлена ошибка приводящая к неработоспособности метода аутентификации radius после обновления версии.
SUM-15253	Исправлена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

Не обнаружено.

Контрольные суммы файлов

Имя файла	MD5	Ufix
siem_x86_update_7.3.0.116739R.bin	aaafc8b361eedb245f9884f64f58eec7	2FEB52FAFBB5B742
siem7-x86-hdd.bz2	b708ef7d4c4167a0e9bb3e944ae9cfdc	99038DE85F403FBD
siem7-x86-hyperv.zip	3e39fb9f72af9276abea0679773a1e0e	9992F5747B81A627

Имя файла	MD5	Ufix
siem7-x86-qcow2.zip	8f3d76d5ac9e2175147603add0c093ff	5E4135C12D17059E
siem7-x86-ovf.zip	94d1015b3a12414c76cdbf2dd980c135	EE945AB97A028DF1

Version: 7.2.x
Product: SIEM
Release Notes: ☒

Статус

Стабильно

Новые возможности

Отсутствуют

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-15253	Исправлена уязвимость, позволяющая получить корневой доступ в систему.
SUM-10195	Исправлена работа генератора отчетов.
SUM-11104	Исправлено отображение поля 'source IP', в журналах web доступа.
SUM-11275	Исправлена работа web интерфейса в закладке 'SOC'.
SUM-11848	Исправлена ошибка формирования отчета, если не указана сортировка в пользовательском шаблоне отчетов.
SUM-11952	Исправлена работа механизма обновления обновляемых списков.
SUM-12848	Исправлена проблема пропадания некоторых событий аутентификации пользователей в UserID, если он размещен на LogAn.
SUM-12849	Исправлена проблема подключения NGFW версий 6.1.x к UserGate LogAn версии 7.2.0.
SUM-12920	Исправлена проблема с зависанием консоли UserID при внесении изменений в UserID connector.
SUM-13148	Исправлена ошибка при использовании команды traceroute в веб-консоли.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-11415	Невозможно удалить сенсор UserGate в веб-консоли.	В следующих версиях ПО.
SUM-12538	Пропадает VLAN на интерфейсах типа bond, при импорте\экспорте конфигурации.	В следующих версиях ПО.

№ задачи	Описание	HotFix
SUM-13565	Некорректное назначение портов в ПАК LogAn.	В следующих версиях ПО.
SUM-13970	После создания 2000 интерфейсов типа vlan могут появиться проблемы с производительностью.	В следующих версиях ПО.
SUM-14275	После обновления с версии 7.1 до 7.2 может перестать работать метод аутентификации радиус.	В следующих версиях ПО.

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	17c0a89b872c1a501c9e80d2fb8912e7	74E38836
logan7-x86-hyperv.zip	5936ec2fa85662de3bf2e85b0f22cd51	BD8656CE
logan7-x86-qcow2.zip	c3a936097a0f481b5c58a40243d298a3	36EA367D
logan7-x86-ovf.zip	839716010a5d54854a47f35835d1734c	D9333F78

Version: 7.3.x
Product: UserGate SIEM
Release Notes: ☒

Статус

Отозвано

Внимание! Версия в стадии бета-тестирования и не рекомендуется для массовой установки в производственную инфраструктуру (production). Задача этой сборки: проверка в "боевых условиях" у лояльных клиентов, сбор обратной связи и выявление потенциальных недостатков на ранней стадии.

Новые возможности

№ задачи	Описание
SUM-7555	Выпущен SIEM в виде отдельного продукта. Logan и SIEM технически разведены для самостоятельного развития в рамках экосистемы SUMMA.
SUM-4859	Добавлена возможность создания кластера отказоустойчивости для SIEM (актив-пассив). Добавлен новый тип узла кластера Арбитратор, обеспечивающий консистентность данных.
SUM-12938	Добавлена библиотека экспертизы правил нормализации для различных источников событий от MRC UserGate, позволяющая оперативно и корректно подключить источники событий в инфраструктуре заказчика. Библиотека нормализации доступна в базовой лицензии продукта.

Улучшения и оптимизации

Отсутствуют.

Исправления

Отсутствуют

Критические изменения в версии

Важно!Введена новая система лицензирования. Теперь SIEM лицензируется по ядрам (эквивалент 1cpu = 1000 Event Per Second). Без лицензии подключение источников недоступно, с активированной лицензией ограничение снимается.

Обновление с предыдущих версий

Важно!Старые инсталляции SIEM 7.1.x 7.2.x нельзя обновлять до нового SIEM 7.3.x , необходима новая инсталляция.

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
siem_x86_update_7.3.0.113300R.bin	19c1577da2e0f6f3488ebef57db9f792	758687C496756392
siem7-x86-hdd.bz2	cc45ec50e8584a1844719d0e9f1347b7	036734C5C12B6666
siem7-x86-hyperv.zip	301b8816ba1c76c360a86f23fbb2be19	F2010E3D61B9D3B5
siem7-x86-qcow2.zip	07976ea62436c063d5af9faa40aeca14	3DAD5091BF8AAFE3
siem7-x86-ovf.zip	71e7efc58332992e3c688adbaaa6e777	FD85DE74B129CBC8

Product: UserGate SIEM
Version: 7.2.0
Release Notes: ☒

Статус

Отозвано

Новые возможности

№ задачи	Описание
SUM-10183	Добавлена возможность использовать поля useragent, mime, url в поисковых запросах.
SUM-10184	Добавлена возможность использования списков IP адресов в поисковых запросах в аналитике и поиске.

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-10195	Исправлена работа генератора отчетов.
SUM-11104	Исправлено отображение поля 'source IP', в журналах web доступа.
SUM-11275	Исправлена работа web интерфейса в закладке 'SOC'.
SUM-11848	Исправлена ошибка формирования отчета, если не указана сортировка в пользовательском шаблоне отчетов.
SUM-11952	Исправлена работа механизма обновления обновляемых списков.
SUM-13148	Исправлена ошибка при использовании команды traceroute в веб-консоли.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	28b2ba54d33837431f9721195f206ad7	A704CB7C
logan7-x86-hyperv.zip	29ef1a1de779368ae5dc7f4da3425ae9	27D3C019

Имя файла	MD5	Ufix
logan7-x86-qcow2.zip	da7dbefc05b57d4c696b456d17a0d7a5	586E5FCB
logan7-x86-ovf.zip	0888fc8a547645bf069ae35ee1675a81	E1245E23
logan_x86_update_7.2.0.76784R.bin	db9969b101a82049e0391b0587966718	F7AA1D10

Version: 7.2.x
Product: UserGate SIEM
Release Notes: ☒

Статус

Бета

Внимание! Версия в стадии бета-тестирования и не рекомендуется для массовой установки в производственную инфраструктуру (production). Задача этой сборки: проверка в "боевых условиях" у лояльных клиентов, сбор обратной связи и выявление потенциальных недостатков на ранней стадии.

Новые возможности

№ задачи	Описание
SUM-10183	Добавлена возможность использовать поля useragent, mime, url в поисковых запросах.
SUM-10184	Добавлена возможность использования списков IP адресов в поисковых запросах в аналитике и поиске.

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-10195	Исправлена работа генератора отчетов.
SUM-11104	Исправлено отображение поля 'source IP', в журналах web доступа.
SUM-11275	Исправлена работа web интерфейса в закладке 'SOC'.
SUM-11848	Исправлена ошибка формирования отчета, если не указана сортировка в пользовательском шаблоне отчетов.
SUM-11952	Исправлена работа механизма обновления обновляемых списков.
SUM-12848	Исправлена проблема пропадания некоторых событий аутентификации пользователей в UserID, если он размещен на LogAn.
SUM-12849	Исправлена проблема подключения NGFW версий 6.1.x к UserGate LogAn версии 7.2.0.
SUM-12920	Исправлена проблема с зависанием консоли UserID при внесении изменений в UserID connector.
SUM-13148	Исправлена ошибка при использовании команды traceroute в веб-консоли.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
----------	----------	--------

№ задачи	Описание	HotFix
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	92680cae1c94237382246a4c599b849a	5E1DDA38
logan7-x86-hyperv.zip	50c30dbd9e2f2d05bbd05b0cbd975706	8DBFB2AD
logan7-x86-qcow2.zip	0d1b64590fd0e1bca5e2fb53ae33a4b0	B5D73FCC
logan7-x86-ovf.zip	80380188b9b0c2a36caaa23e603e1a4a	D3218965
logan_x86_update_7.2.0.70211R.bin	21a2932175f465ed339829a57e58e4f3	5E0D6501

Version: 7.2.x
Product: UserGate SIEM
Release Notes: ☒

Статус

Отозвано

Новые возможности

№ задачи	Описание
SUM-10183	Добавлена возможность использовать поля useragent, mime, url в поисковых запросах.
SUM-10184	Добавлена возможность использования списков IP адресов в поисковых запросах в аналитике и поиске.

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-10195	Исправлена работа генератора отчетов.
SUM-11104	Исправлено отображение поля 'source IP', в журналах web доступа.
SUM-11275	Исправлена работа web интерфейса в закладке 'SOC'.
SUM-11848	Исправлена ошибка формирования отчета, если не указана сортировка в пользовательском шаблоне отчетов.
SUM-11952	Исправлена работа механизма обновления обновляемых списков.
SUM-12848	Исправлена проблема пропадания некоторых событий аутентификации пользователей в UserID, если он размещен на LogAn.
SUM-12849	Исправлена проблема подключения NGFW версий 6.1.x к UserGate LogAn версии 7.2.0.
SUM-12920	Исправлена проблема с зависанием консоли UserID при внесении изменений в UserID connector.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
-----------	-----	------

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	655ee2370f7841bbf8fd9045382bb5fe	9AAE2BB8
logan7-x86-hyperv.zip	be028b4eb89b7c4a470c3f72cd464963	BDD6B44C
logan7-x86-qcow2.zip	af9eb82ef010ff59a658eec4924230d7	C60DCA84
logan7-x86-ovf.zip	dd9fa509eb3dc6d1af43091aced2f120	643FC1F7
logan_x86_update_7.2.0.67150R.bin	dbf55008b0e686fcb66c86aa9fccd18f	51C78D65

Version: 7.x
Product: UserGate SIEM
Release Notes: ☒

Статус

Отозвано

Новые возможности

№ задачи	Описание
SUM-10183	Добавлена возможность использовать поля useragent, mime, url в поисковых запросах.
SUM-10184	Добавлена возможность использования списков IP адресов в поисковых запросах в аналитике и поиске.

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
SUM-10195	Исправлена работа генератора отчетов.
SUM-11104	Исправлено отображение поля 'source IP', в журналах web доступа.
SUM-11275	Исправлена работа web интерфейса в закладке 'SOC'.
SUM-11848	Исправлена ошибка формирования отчета, если не указана сортировка в пользовательском шаблоне отчетов.
SUM-11952	Исправлена работа механизма обновления обновляемых списков.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

>

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	593d7d5efa8df099b42e5a2ea805689a	6213120D
logan7-x86-hyperv.zip	74c635c9deaf178647468de8803dec2c	B3DB1366
logan7-x86-qcow2.zip	6a69f2f24ebfe32449b84d2f39f9ab5c	E561497F

Имя файла	MD5	Ufix
logan7-x86-ovf.zip	67501523393c3fafc238f00013c13115	0E064265
logan_x86_update_7.2.0.60375R.bin	6c02dc8cd32fd1d3d3ace011a8ba26b3	0A2EAFC2

Version: 7.1.x
Product: UserGate SIEM
Release Notes: ☒

Статус

Стабильно

Новые возможности

- Отсутствуют

Улучшения и оптимизации

№ задачи	Описание
SUM-8969	Улучшена отрисовка виджетов.

Исправления

№ задачи	Описание
SUM-10047	Исправлено отображение информации о RAID в виджетах рабочего стола и в CLI.
SUM-10542	Добавлена возможность передачи состояния RAID по SNMP.
SUM-11041	Исправлена невозможность открыть конфигурацию syslog сервера после обновления.
SUM-32	Введен запрет на добавление в кластер отказоустойчивости интерфейсов без назначенного IP адреса.
SUM-5524	Добавлена возможность настройки интервала запуска правил аналитики в автоматическом режиме.
SUM-8649	Исправлена ошибка с правами администратора с корневым профилем.
SUM-9288	Исправлена работа узлов кластера с SNMP.
SUM-9682	Добавлены события успешной загрузки устройства в журнал событий.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Важно! Для корректного обновления кластера NGFW с предыдущих версий необходимо дождаться завершения обновления первого узла и только после этого начинать процедуру обновления остальных узлов кластера. Нарушение данного требования может привести к невозможности загрузки последующих узлов после завершения процедуры их обновления.

Поддерживается обновление на версию 7.1.2 только с версий:

- 7.1.x - штатными средствами "по воздуху". Переустановка системы не требуется.
- 7.0.1 - через процедуру экспорта настроек, установки системы с нуля и импорта настроек.
- 6.1.9 - через процедуру экспорта настроек, установки системы с нуля и импорта настроек.

Важно!Обновление с версий, выпущенных до 6.1.9, **НЕ ПОДДЕРЖИВАЕТСЯ!** Необходимо сначала обновиться до последней 6.1.9 и затем производить переход на версию 7.1.2.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-10195	Возможно аварийное завершение генератора отчетов.	-

№ задачи	Описание	HotFix
SUM-11104	В журнале web доступа в качестве 'source ip' может отображаться 127.0.0.1, вместо IP адреса пользователя.	-
SUM-11275	Некорректная работа web интерфейса в закладке 'SOC'.	-
SUM-11848	Возникает ошибка если при создании пользовательского шаблона отчётов не указать сортировку.	-
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	e10fd3321559de4094393bb43baf9508	702B3191
logan7-x86-hyperv.zip	0fae0eefa61d8b2f615f32344a6d9683	EBC27E7F
logan7-x86-qcow2.zip	c4e8ad7f9696179fbaac9ebe5b3c7b4b	3BC5D607
logan7-x86-ovf.zip	436d641132bc07f9cef6facdb626cb00	0E477E8B
logan_x86_update_7.1.2.33025R.bin	6bab301cfa7c13022af1588062a9ec3d	D1C9FE9A

Version: 7.1.x
Product: UserGate SIEM
Release Notes: ☒

Статус

Бета

Новые возможности

- Отсутствуют

Улучшения и оптимизации

№ задачи	Описание
SUM-8969	Улучшена отрисовка виджетов.

Исправления

№ задачи	Описание
SUM-10047	Исправлено отображение информации о RAID в виджетах рабочего стола и в CLI.
SUM-10542	Добавлена возможность передачи состояния RAID по SNMP.
SUM-32	Введен запрет на добавление в кластер отказоустойчивости интерфейсов без назначенного IP адреса.
SUM-5524	Добавлена возможность настройки интервала запуска правил аналитики в автоматическом режиме.
SUM-8649	Исправлена ошибка с правами администратора с корневым профилем.
SUM-9288	Исправлена работа узлов кластера с SNMP.
SUM-9682	Добавлены события успешной загрузки устройства в журнал событий.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Поддерживается обновление на версию 7.1.2 только с версий:

- 7.1.x - штатными средствами "по воздуху". Переустановка системы не требуется.
- 7.0.1 - через процедуру экспорта настроек, установки системы с нуля и импорта настроек.
- 6.1.9 - через процедуру экспорта настроек, установки системы с нуля и импорта настроек.

Важно!Обновление с версий, выпущенных до 6.1.9, **НЕ ПОДДЕРЖИВАЕТСЯ!** Необходимо сначала обновиться до последней 6.1.9 и затем производить переход на версию 7.1.2.
Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
-----------	-----	------

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	58d9a2f00485d5e9a20db0adc5849e5c	54513248
logan7-x86-hyperv.zip	a8b9360d386ebaaebec06bca8d18d233	4C27CA73
logan7-x86-qcow2.zip	d900ca052ebc68c3961e1a554c46363a	00DCC059
logan7-x86-ovf.zip	7e07fba1cdd32c131ba4925f65c66950	1EAB76E5
logan_x86_update_7.1.2.30045R.bin	1db40cb1c76306d988bb13e7511ad0c4	D6BFC2EB

Version: 7.x
Product: SIEM
Release Notes: ☒

Статус

Стабильно

Новые возможности

- Отсутствуют

Улучшения и оптимизации

№ задачи	Описание
SUM-8847	Добавлена настройка radmin в CLI.

Исправления

№ задачи	Описание
SUM-1226	Исправлена работа механизма создания вложенных списков.
SUM-7675	Исправлено отображение кириллических доменов в журнале событий.
SUM-7679	Исправлены ошибки импорта правил аналитики из файла YAML, возникающие при наличии одинарных кавычек в запросе фильтра.
SUM-7847	Исправлено отображение хэша в уликах при создании инцидента.
SUM-7964	Исправлена синхронизация SNMPv3 правил из MC.
SUM-7972	Исправлено некорректное отображение данных по использованию RAM на графике производительности в Дашборд.
SUM-7972	Исправлено некорректное отображение данных по использованию RAM на графике производительности в Дашборд.
SUM-8102	Исправлено некорректное отображение дерева процессов конечных устройств.
SUM-8165	Исправлены ошибки в профилях администратора.
SUM-8194	Исправлено некорректное отображение записи журнала событий об активации лицензии с ограничением по количеству CPU.
SUM-8258	Исправлены ошибки отображения информации о конечных устройствах в CLI.
SUM-8373	Исправлена работа пользовательского отчета.
SUM-8475	Исправлена ошибка при которой не показывался тип интерфейса с установленным признаком 'Configured on the device'.
SUM-8555	Исправлена работа механизма изменения сенсора.
SUM-8571	Исправлена ошибка, связанная с невозможностью удаления профилей оповещения.
SUM-8588	Исправлены ошибки, возникавшие при создании правил отчётов.
SUM-8594	Исправлена ошибка назначения прав доступа для администратора LogAn через профиль администратора.

№ задачи	Описание
SUM-8639	Исправлена ошибка недостаточности прав при редактировании профиля оповещений.
SUM-8643	Исправлено редактирование списков адресов электронной почты в профиле оповещений администратора.
SUM-8764	Исправлено взаимодействие CLI с выключенными сенсорами Log Analyzer.
SUM-8885	Исправлена работа виджета 'график сенсора'.
SUM-8887	Исправлены проблемы совместимости между Log Analyzer v7.1.0 и более ранними NGFW.
SUM-9160	Исправлены ошибки отображения записей журнала событий об изменениях настроек администраторов.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-10047	Не отображается информация о RAID в виджетах рабочего стола и в CLI.	По запросу в службу поддержки
SUM-11041	После обновления, в правила syslog коллектора невозможно открыть конфигурацию syslog сервера.	По запросу в службу поддержки
SUM-8649	Администратор с корневым профилем может создать инцидент, но не может выполнить некоторые операции по его модификации.	По запросу в службу поддержки
SUM-9288	Некорректная работа улов кластера с SNMP.	По запросу в службу поддержки
SUM-9682	В журнале событий не фиксируется событие успешной загрузки устройства.	По запросу в службу поддержки
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	086d4372853fb603bdeb9b465d4917b5	4688280E
logan7-x86-hyperv.zip	b213d9285fc40d021805ebd9a076a7cc	65019AC8
logan7-x86-qcow2.zip	8de7c01cb047b0faf4de8f00129bd659	89E437F0
logan7-x86-ovf.zip	f461907aa62612654fa21b35dc43d21c	43339DAF
logan_x86_update_7.1.1.12162R.bin	ecae1c224762d806f2f14c0a05f157a6	0A3AD8AE

Product: SIEM
Release Notes: ☒
Version: 7.1.0

Статус

Стабильно

Новые возможности

№ задачи	Описание
SUM-3222	Добавлена возможность автоматического реагирования на инциденты безопасности в виде отправки команды на конечное устройство.
SUM-3265	Добавлена возможность задать адрес Management Center и LogAnalyzer/SIEM с помощью FQDN.
SUM-3444	Добавлена возможность просмотра размера заполненного диска и настройки периода хранения журналов событий.
SUM-4313	Добавлена поддержка устройств UserGate LogAn для централизованного управления.
SUM-4499	Добавлена пользовательская нормализация записей журналов событий конечных устройств и Syslog.
SUM-4855	Добавлен функционал SIEM (Security Information and Event Management).
SUM-4855	Добавлен функционал IRP (Incident Response Platform).
SUM-4855	Добавлено разделение полей UserGate Log Analyzer на Log Collector и SIEM.
SUM-4872	Добавлена возможность использования данных, полученных с конечных устройств, при построении общей картины состояния безопасности на предприятии, корреляция данных с другими источниками данных.
SUM-4872	Добавлена поддержка конечных устройств с установленным ПО UserGate Client в качестве источника информации.Добавлено получение телеметрической информации конечных устройств (загрузка ресурсов, списки запущенных процессов и служб), журналов Windows, другой существенной информации о безопасности конечных устройств.
SUM-6755	Добавлены возможности представления информации (дрилл-дауны, удобное построение фильтров отображения информации) в журналах и в Дашборде.

Улучшения и оптимизации

Отсутствуют

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-1226	Некорректная работа механизма создания вложенных списков.	По запросу в службу поддержки
SUM-7675	Некорректно отображаются кириллические домены в журнале событий.	По запросу в службу поддержки

№ задачи	Описание	HotFix
SUM-7679	Наблюдаются ошибки при импорте правил аналитики из файла YAML, возникающие при наличии одинарных кавычек в запросе фильтра.	По запросу в службу поддержки
SUM-7847	Некорректно отображается значение хэша в уликах, при создании инцидента.	По запросу в службу поддержки
SUM-7964	Синхронизация SNMPv3 правил из MC отключает локальные SNMPv3 правила.	По запросу в службу поддержки
SUM-7972	Некорректно отображаются данные по использованию RAM на графике производительности в Дашборд.	По запросу в службу поддержки
SUM-8102	Некорректно отображается дерево процессов конечных устройств.	По запросу в службу поддержки
SUM-8165	Отсутствуют некоторые пункты в настройках профиля администратора.	По запросу в службу поддержки
SUM-8194	В журнале событий некорректно отображается информация об активации лицензии с ограничением по количеству CPU.	По запросу в службу поддержки
SUM-8258	Возникают ошибки при запросе информации о конечных устройствах в CLI.	По запросу в службу поддержки
SUM-8373	При создании пользовательского отчета может выдаваться ложное сообщение об отсутствии в шаблоне некоторого поля\полей.	По запросу в службу поддержки
SUM-8475	При создании сетевых интерфейсов с включенным чекбоксом 'Configured on the device', в дальнейшем не показывается их тип.	По запросу в службу поддержки
SUM-8555	Некорректно работает механизм изменения сенсора.	По запросу в службу поддержки
SUM-8571	Некорректно работает механизм удаления профилей оповещения.	По запросу в службу поддержки
SUM-8588	Ошибки при создании правил отчетов.	По запросу в службу поддержки
SUM-8594	Ошибка при назначении прав доступа для администратора LogAn через профиль администратора.	По запросу в службу поддержки
SUM-8639	При создании SMPP профиля в правиле оповещений возникает ошибка 'Не хватает прав доступа'.	По запросу в службу поддержки
SUM-8643	Невозможно редактировать списки адресов электронной почты в правиле оповещения для соответствующего профиля администратора.	По запросу в службу поддержки
SUM-8764	Возникает внутренняя ошибка CLI при попытке обратиться к выключенному сенсору Log Analyzer.	По запросу в службу поддержки
SUM-8847	Отсутствует возможность настройки режима удаленного помощника в CLI.	По запросу в службу поддержки
SUM-8885	Некорректная работа виджета 'график сенсора'.	По запросу в службу поддержки
SUM-8887	Существует проблема совместимости между Log Analyzer v7.1.0 и более ранними версиями NGFW.	По запросу в службу поддержки
SUM-9160	Некорректно отображается информация об изменении настроек администраторов в записях журнала событий.	По запросу в службу поддержки
SUM-943	Некорректно работает импорт списков библиотек.	По запросу в службу поддержки
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	0fb65a1e43a559d4801b1c5f02afa62b	9E47EDEE
logan7-x86-hyperv.zip	6cdeaf3f14de612bfa1ef021a6c0419b	BFA54ACE
logan7-x86-qcow2.zip	7b3927606566b7f42db25d6e7ba966af	F83146A2
logan7-x86-ovf.zip	14e3025692b9c14e0aab06993f1e7604	1FCFC521

Version: 7.1.0
Product: LogAn, SIEM
Release Notes: ☒

Статус

Release Candidat

Новые возможности

- Отсутствуют

Улучшения и оптимизации

№ задачи	Описание
SUM-2782	Улучшена работа правил нормализации.

Исправления

№ задачи	Описание
SUM-2874	Исправлены ошибки в работе Web-интерфейса UserGate Log Analyzer.
SUM-2904	Убрана возможность удалить на всех шлюзах метку 'default'.
SUM-3021	Исправлена работа модуля редактирования SNMP профиля безопасности.
SUM-3037	SSH backup: Исправлена проверка SSH соединения.

Критические изменения в версии

Внимание! Не рекомендуется использовать данную версию в промышленной эксплуатации.

Обновление с предыдущих версий

ВниманиеОбновления в Release Candidat не предусмотрены.

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	460018b954455bb12447498782008112	E00B3571
logan7-x86-hyperv.zip	5c306130f62fbfea4322488986e7fc2c	398E97AD
logan7-x86-qcow2.zip	8dcde2461174d319f9e653ad86e8976a	AA05655D
logan7-x86-ovf.zip	abf3c205d25caaa1140e973e9feffc20	6663A32F

Version: 7.1.0
Product: UserGate SIEM
Release Notes: ☒

Статус

Release Candidate

Новые возможности

№ задачи	Описание
UGDNS-11377	Добавлена возможность автоматического реагирования на инциденты безопасности в виде отправки команды на конечное устройство.
UGDNS-12561	Добавлена возможность использования данных, полученных с конечных устройств, при построении общей картины состояния безопасности на предприятии, корреляция данных с другими источниками данных.
UGDNS-12590	Добавлено получение телеметрической информации конечных устройств (загрузка ресурсов, списки запущенных процессов и служб), журналов Windows, другой существенной информации о безопасности конечных устройств.
UGDNS-15517	Добавлен функционал UserID для осуществления прозрачной аутентификации по журналам Active Directory и Syslog.
UGDNS-15896	Оптимизирован процесс добавления срабатываний правила аналитики в инцидент, если в качестве действия реагирования указано создание инцидента.
UGDNS-18146	Добавлена возможность получения событий Unix-систем по протоколам TCP и UDP одновременно.
UGDNS-19552	Добавлено разделение полей UserGate Log Analyzer на Log Collector и SIEM.
UGDNS-19592	Добавлены новые модули лицензирования, предоставляющие доступ к функционалу SIEM и обновлению соответствующих библиотек.
UGDNS-18674	Добавлено отображение в веб-консоли уведомлений о срабатываниях правил аналитики.
UGDNS-18775	Расширен функционал CLI и PMC CLI.

Критические изменения в версии

Внимание! Не рекомендуется использовать данную версию в промышленной эксплуатации.

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	ce0235b61527225aecfa755b81638345	6B971395
logan7-x86-hyperv.zip	81dae524069edef07664435f309dd352	5CCED576
logan7-x86-qcow2.zip	f6baace48249fa38f37ee9816a4686ee	7EC1CD1A
logan7-x86-ovf.zip	7b612bdb906133646976a58103422482	01F46E2F

Имя файла	MD5	Ufix
logan_x64_update_7.1.0.1605R.bin	7b612bdb906133646976a58103422482	01F46E2F

Version: 7.0.1
Release Notes: ☒

Статус

Бета

Новые возможности

- Отсутствуют

Улучшения и оптимизации

Отсутствуют.

Исправления

Технический выпуск. Исправления отсутствуют.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
SUM-8649	Администратор с корневым профилем может создать инцидент, но не может выполнить некоторые операции по его модификации.	По запросу в службу поддержки.
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	8419e5ebff4adfd2d30d617420e1825e	602D88A5
logan7-x86-hyperv.zip	16022bcfb0c50693fa90c7f81d5ad59a	91D8326B
logan7-x86-qcow2.zip	5a7286dcf5047b2323e686a7c7063b48	9B7A59B8
logan7-x86-ovf.zip	7ca1ed804ec2d1040206efcd2133a798	4D06F526
logan_x64_update_7.0.1.1052R.bin	db2e4c82fe2a04a9b36a95b8287fcac9	7E89CD75

Version: 7.0.1
Product: SIEM
Release Notes: ☒

Статус

Стабильно

Новые возможности

- Отсутствуют

Улучшения и оптимизации

Отсутствуют.

Исправления

Технический выпуск. Исправления отсутствуют.

Критические изменения в версии

Отсутствуют

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
UGDNS-15145	В свойствах LDAP-коннектора проверяется keytab-файл, хотя он не загружается в LogAn и MC.	
UGDNS-15731	Некорректно работает импорт конфигурации с версии 6.1.x на 7.x	
UGDNS-17880	При создании действия реагирования типа «Создать инцидент» не сохраняется список наблюдателей.	
UGDNS-18478	При добавлении администратора посредством LDAP-сервера с именем на кириллице, в журналах это имя отображается некорректно.	
UGDNS-20199	Невозможна оффлайн активация LogAn из-за ошибки Web-интерфейса.	
UGDNS-20947	При запуске преднастроенного отчета 'Webaccess detailed report' возникает ошибка 'Invalid query'.	
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	6932331358e9f526407f652b0be06b98	D339E61C
logan7-x86-hyperv.zip	30c3878135228e5d1745bfcbb3e6d672	9E5B3D20
logan7-x86-qcow2.zip	4d70044b6d235d8995c81dc77f1b09c8	C3663A7F

Имя файла	MD5	Ufix
logan7-x86-ovf.zip	855c58696e62fabfdca83d9b2b0cadd8	D3F1E957
logan_x64_update_7.0.1.1051R.bin	008e5f989ce33b419359cd9d93252eed	CD0E102A

Version: 7.0.1
Product: LogAn, SIEM
Release Notes: ☒

Внимание!Для платформ C150 обновление на версии ниже этой следует производить вручную. Обновление "по воздуху" может привести к неработоспособности устройства.

Статус

Отозван

Новые возможности

- Отсутствуют

Улучшения и оптимизации

Отсутствуют.

Исправления

Технический выпуск. Исправления отсутствуют.

Критические изменения в версии

Внимание!В данной версии произведены критические изменения - обновление на эту версию возможно только с версии 7.0.1.1022R! Обновления с более ранних версий на эту недоступны!

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
UGDNS-15145	В свойствах LDAP-коннектора проверяется keytab-файл, хотя он не загружается в LogAn и MC.	
UGDNS-15731	Некорректно работает импорт конфигурации с версии 6.1.x на 7.x	
UGDNS-17880	При создании действия реагирования типа «Создать инцидент» не сохраняется список наблюдателей.	
UGDNS-18478	При добавлении администратора посредством LDAP-сервера с именем на кириллице, в журналах это имя отображается некорректно.	
UGDNS-20199	Невозможна оффлайн активация LogAn из-за ошибки Web-интерфейса.	
UGDNS-20947	При запуске преднастроенного отчета 'Webaccess detailed report' возникает ошибка 'Invalid query'.	
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	e7e12440d491c0384a2b25f253a5da3c	776978A1
logan7-x86-hyperv.zip	9af009ee1127458324f96822f79155ad	4C109F5C
logan7-x86-qcow2.zip	f2b653431ea70d833e00f51e384bd658	A4790BD0

Имя файла	MD5	Ufix
logan7-x86-ovf.zip	3d215b4e816946cd8b53854a5c5055bb	CC41C4CE
logan_x64_update_7.0.1.1043R.bin	8ff3088fe87710f0acf4ba517b857899	8DB37713

Version: 7.0.1
Product: UserGate LogAn
Release Notes: ☒

Внимание!Для платформ C150 обновление на версии ниже 7.0.1.1043R следует производить вручную. Обновление "по воздуху" может привести к неработоспособности устройства.

Статус

Стабильно

Новые возможности

- Отсутствуют

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
UGDNS-21315	Исправлена ошибка в механизме обновления ARM версии, которая могла привести к неработоспособности устройства.

Критические изменения в версии

Внимание!В данной версии произведены критические изменения - дальнейшие обновления будут возможны только с этой версии!
Обновления с ранних версий на последующие недоступны, таким образом данная версия обязательна к установке!

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
UGDNS-15145	В свойствах LDAP-коннектора проверяется keytab-файл, хотя он не загружается в LogAn и MC.	
UGDNS-15731	Некорректно работает импорт конфигурации с версии 6.1.x на 7.x	
UGDNS-17880	При создании действия реагирования типа «Создать инцидент» не сохраняется список наблюдателей.	
UGDNS-18478	При добавлении администратора посредством LDAP-сервера с именем на кириллице, в журналах это имя отображается некорректно.	
UGDNS-20199	Невозможна офлайн активация LogAn из-за ошибки Web-интерфейса.	
UGDNS-20947	При запуске преднастроенного отчета 'Webaccess detailed report' возникает ошибка 'Invalid query'.	
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	bf227d2ccec364b69ecb1bfb558bfc51	574B4125
logan7-x86-hyperv.zip	e8a24e6b451e9f03e7dd3f90cf040892	C8D5B59E

Имя файла	MD5	Ufix
logan7-x86-qcow2.zip	83e0a4ed70a541d3bd1608f81a0e4b57	48A99FE9
logan7-x86-ovf.zip	eefecc8041e8a96398101b71450301d8	B0ACA1C5
logan_x64_update_7.0.1.1022R.bin	f5fb6ab89c46c32d0778cd95c19de509	0BEA7C58

Version: 7.0.1
Product: UserGate LogAn, UserGate SIEM
Release Notes: ☒

Статус

Отозван

Новые возможности

- Отсутствуют

Улучшения и оптимизации

Отсутствуют.

Исправления

№ задачи	Описание
UGDNS-21315	Исправлена ошибка в механизме обновления модели C150, которая могла привести к неработоспособности устройства.

Критические изменения в версии

Внимание!В данной версии произведены критические изменения - дальнейшие обновления будут возможны только с этой версии!
Обновления с ранних версий на последующие недоступны, таким образом данная версия обязательна к установке!

Обновление с предыдущих версий

Обновление с предыдущих версий производится штатными средствами.

Важно! Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

Известные ошибки и недочеты

№ задачи	Описание	HotFix
UGDNS-15145	В свойствах LDAP-коннектора проверяется keytab-файл, хотя он не загружается в LogAn и MC.	
UGDNS-15731	Некорректно работает импорт конфигурации с версии 6.1.x на 7.x	
UGDNS-17880	При создании действия реагирования типа «Создать инцидент» не сохраняется список наблюдателей.	
UGDNS-18478	При добавлении администратора посредством LDAP-сервера с именем на кириллице, в журналах это имя отображается некорректно.	
UGDNS-20199	Невозможна офлайн активация LogAn из-за ошибки Web-интерфейса.	
UGDNS-20947	При запуске преднастроенного отчета 'Webaccess detailed report' возникает ошибка 'Invalid query'.	
SUM-15253	Найдена уязвимость, позволяющая при наличии административного доступа в web консоль администратора, выполнять произвольные команды на уровне ОС.	В версиях выше 7.2.1 и 7.3.0.116739R включительно

Контрольные суммы файлов

Имя файла	MD5	Ufix
logan7-x86-hdd.bz2	e4687333b93558fc8b12445f0b05cd22	0F1319AF
logan7-x86-hyperv.zip	5687b274b32fc635e07dca6f500ab25a	4019A131
logan7-x86-qcow2.zip	6ffb632249ee8b4edd48a9a6c0ae8dcd	BD7E76DF

Имя файла	MD5	Ufix
logan7-x86-ovf.zip	c0f7b111e6fd26ea4edca45cb90c8006	227AA0BB
logan_x64_update_7.0.1.1020R.bin	bfd439503081e1c62860971dacc0958c	4ED383FE

