АО «Лаборатория Касперского»

Бюллетень

643.46856491.23БЭ

2016

Введение

Бюллетень распространяется на программное изделие «Антивирус Касперского для Proxy Server 5.5» (643.46856491.00047-02).

Основанием для выпуска данного бюллетеня является извещение об изменении 643.46856491.02-2016.

Срок введения в действие: февраль 2016 г.

Номер изменения: 1.

АО «Лаборатория Касперского» заявляет соответствие программного изделия «Антивирус Касперского для Proxy Server 5.5» (643.46856491.00047-02) требованиям методического документа ФСТЭК «Профиль защиты средств антивирусной защиты типа «Б» второго класса защиты» ИТ.САВЗ.Б2.ПЗ.

Изменения вносятся в соответствии с ГОСТ 19.604-78.

Версии документов с внесенными изменениями включены в комплект поставки программного изделия с переоформленным сертификатом соответствия.

1 Внесение изменений

1.1. Изменения в формуляр 643.46856491.00047-02 30 01 вносятся согласно приложению к настоящему бюллетеню.
1.2. Предшествующие бюллетени, в соответствии с которыми вносились предыдущие изменения в документацию программного изделия: 643.46856491.08БЭ.

2 Приложение (содержание изменений)

2.1. Исправить «ЗАО «Лаборатория Касперского» на «АО «Лаборатория Касперского».
2.2. Удалить п.1.6 раздела 1.
2.3. Дополнить раздел 2 пунктами 2.3 и 2.4 следующего содержания:

2.3 Программное изделие «Антивирус Касперского для Proxy Server 5.5» является средством антивирусной защиты и предназначено для защиты от вредоносных компьютерных программ, в том числе в системах обработки данных и государственных информационных системах органов государственной власти Российской Федерации.

2.4 В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, введенными в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г., и Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, введенными в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г., изделие может использоваться в информационных системах 1 и 2

класса защищенности и для обеспечения защищенности персональных данных до 1 уровня включительно.

2.4. Заменить таблицу 1 раздела 3 следующей:

№ пп	Имя файла	Дата создания	Длина, байт	КС
Каталог D:				
1	release_notes_kav4proxy_mp3cf1_en.txt	26.06.12 11-04	5974	36b4aaec426cfa5de74cb9b74c4849a4bd5442b3f8e212932c4b2ca065c97d7a
2	release_notes_kav4proxy_mp3cf1_ru.txt	26.06.12 11-04	6206	baeaec9112bef76107aff74a556e9a333e830c757d2eb7a15421e4c766c6c845
итого: файлов - 2			**12180**	**8c5e467d50d20d3ce0e34efd1926d39783d74ec685cca532786ac867030fb53f**
Каталог D:\doc				
3	kav5.5mp3cf1_proxy_ru (rev.2016).pdf	27.04.16 16-50	1066854	3104cb13e98aec2ee72e3e3b8a2a1a3efae6643d8aecbe5b6c3a96e8a79116f1
итого: файлов - 1			**1066854**	**3104cb13e98aec2ee72e3e3b8a2a1a3efae6643d8aecbe5b6c3a96e8a79116f1**
Каталог D:\freebsd-7.x				
4	kav4proxy-5.5_86.tgz	19.06.12 19-21	5666675	e84b67bb15d6f100de370fc173909bf9d22466ec1f1d6886370439a3cfa3dee8
итого: файлов - 1			**5666675**	**e84b67bb15d6f100de370fc173909bf9d22466ec1f1d6886370439a3cfa3dee8**
Каталог D:\freebsd-8.x				
5	kav4proxy-5.5_86.tgz	19.06.12 19-22	5666667	cd2f3e69f726fecae6dbd62e34d9ecc97a2bb79959a0b19d0ecf45e665731604
итого: файлов - 1			**5666667**	**cd2f3e69f726fecae6dbd62e34d9ecc97a2bb79959a0b19d0ecf45e665731604**
Каталог D:\freebsd-9.x				
6	kav4proxy-5.5_86.tgz	19.06.12 19-21	5662801	0380614c744b0039932c1438e92c2f9730a018096585226c957bd6fe47702984
итого: файлов - 1			**5662801**	**0380614c744b0039932c1438e92c2f9730a018096585226c957bd6fe47702984**
Каталог D:\linux				
7	kav4proxy-5.5-86.i386.rpm	19.06.12 19-20	5934920	e1bb2df79141c4f073e0f7041940e7148e6cc59bb03fa10a77c27ee0f390f490
8	kav4proxy_5.5-86_i386.deb	19.06.12 19-21	5867308	f92e1d85a70004feb7263c014859469149f1fd5886f20b100b9504c6a8c20f4c
итого: файлов - 2			**11802228**	**189530723641c00ec4c6cb055119a185c79d38c336cdaa1a7c577a265b52fbdc**
ВСЕГО: файлов - 8			**29877405**	**832b858219a22eef68cb76146c70308b2603db441ad54a04c4b78e12126cb97a**
Конец				

2.5. Заменить текст раздела 4 следующим:

«4.1 Реализованные в программном изделии функции безопасности (АВ3.1, АВ3.2) :

4.1.1 Аудит безопасности:

а) возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;

б) возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;

в) возможность читать информацию из записей аудита;

г) ограничение доступа к чтению записей аудита;

д) поиск данных аудита;

4.1.2 Управление безопасностью:

а) возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности САВЗ;

б) возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;

в) поддержка определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и пользователями ИС.

4.1.3 Проверки объектов заражения:

а) возможность выполнять проверки с целью обнаружения зараженных ВКПВ объектов;

б) возможность выполнения проверок с целью обнаружения зараженных ВКПВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных.

4.1.4 Методы проверок объектов заражения:

а) возможность выполнять проверки с целью обнаружения зараженных ВКПВ объектов сигнатурными и эвристическими методами;

б) возможность выполнять проверки с целью обнаружения зараженных ВКПВ объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;

в) возможность выполнять проверки с целью обнаружения зараженных ВКПВ объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой;

4.1.5 Обработка объектов, подвергшихся воздействию:

а) возможность удаления (если удаление технически возможно) файлов, в которых обнаружены ВКПВ, а также файлов, подозрительных на наличие ВКПВ, перемещение и изолирование объектов воздействия;

4.1.6 Блокирование:

а) возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных ВКПВ, сервера, на котором обнаружены зараженные файлы;

4.1.7 Сигнализация:

а) возможность отображения сигнала тревоги на АРМ администратора, в том числе до подтверждения его получения или до завершения сеанса;

4.1.8 Восстановление объектов:

а) возможность восстановления функциональных свойств зараженных объектов;

4.1.9 Обновление базы данных ПВКПВ:

а) возможность получения и установки обновлений БД ПВКПВ без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса.»

2.6. Дополнить список «64-битные платформы» подпункта 6.1.2 раздела 6 следующим элементом:

- *Astra Linux SE 1.4 (только при отключенном механизме мандатного разграничения доступа и отключенном механизме создания замкнутой программной среды).*

2.7. Дополнить текст п. 6.4 следующим:

«Прошедшие инспекционный контроль обновления программных компонентов необходимо получать путем обращения в техническую поддержку АО «Лаборатория Касперского».

2.8. Удалить п. 6.6.