ФСТЭК РОССИИ
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПО ПРИВОЛЖСКОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ

Гагарина просп., д. 60, корп. 11,
г. Нижний Новгород, 603104
тел./факс (831) 439 – 68 – 79

«11» ноября 2022 г.
№ 3-2/1001

Заместителю
Председателя Правительства
Республики Марий Эл
С.А.ВОРОНЦОВУ

О дополнительных мерах
по повышению защищенности
информационной инфраструктуры

Уважаемый Степан Александрович!

Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками при реализации компьютерных атак на информационную инфраструктуру Российской Федерации активно эксплуатируются уязвимости программного обеспечения.

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, прошу Ваших указаний на устранение следующих уязвимостей:

1. Уязвимость реализации протокола Kerberos операционных систем Windows (BDU:2022-02861, уровень опасности: по CVSS 2.0 высокий уровень опасности, по CVSS 3.0 высокий уровень опасности), связанной с ошибками управления привилегиями. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения при условии выполнения рекомендаций Управления ФСТЭК России по Приволжскому федеральному округу от 12 мая 2022 г. № Э-2/444.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

для Windows Server 2012 и более поздних версий применить безопасное туннелирование гибкой аутентификации (FAST) с целью предотвращения эксплуатации уязвимости;

отключить параметр «Не требовать предварительной аутентификации Kerberos».

2. Уязвимость утилиты ntfs-3g набора драйверов NTFS-3G реализации файловой системы NTFS (BDU:2022-06607, уровень опасности: по CVSS 2.0 средний уровень опасности, по CVSS 3.0 высокий уровень опасности), связанная с ошибками при обработке метаданных. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения при условии выполнения рекомендаций Управления ФСТЭК России по Приволжскому федеральному округу от 12 мая 2022 г. № Э-2/444.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

отключить возможность автоматического монтирования NTFS-разделов;

ограничить возможность подключения недоверенных USB-устройств.

3. Уязвимость функционала проверки сертификата X.509 библиотеки OpenSSL (BDU:2022-06608, уровень опасности: по CVSS 2.0 критический уровень опасности, по CVSS 3.0 критический уровень опасности), связанная с переполнением буфера в стеке. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения при условии выполнения рекомендаций Управления ФСТЭК России по Приволжскому федеральному округу от 12 мая 2022 г. № Э-2/444.

В случае невозможности установки обновления программного обеспечения необходимо использовать средства межсетевого экранирования с целью ограничения доступа к недоверенным ресурсам.

4. Уязвимость функционала проверки сертификата X.509 библиотеки OpenSSL (BDU:2022-06609, уровень опасности: по CVSS 2.0 высокий уровень

опасности, по CVSS 3.0 высокий уровень опасности), связанная с переполнением буфера в стеке. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, аварийно завершить работу приложения.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения при условии выполнения рекомендаций Управления ФСТЭК России по Приволжскому федеральному округу от 12 мая 2022 г. № Э-2/444.

В случае невозможности установки обновления программного обеспечения необходимо использовать средства межсетевого экранирования с целью ограничения доступа к недоверенным ресурсам.

5. Уязвимость в файле plugins/sudoers/auth/passwd.c программы системного администрирования Sudo (BDU:2022-06664, уровень опасности: по CVSS 2.0 средний уровень опасности, по CVSS 3.0 высокий уровень опасности), связанной с возможностью чтения за пределами буфера в памяти. Эксплуатация указанной уязвимости может позволить нарушителю вызвать отказ в обслуживании.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения при условии выполнения рекомендаций Управления ФСТЭК России по Приволжскому федеральному округу от 12 мая 2022 г. № Э-2/444.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей;

принудительно сменить пароли пользователей;

ограничить доступ к командной строке для недоверенных пользователей;

использовать антивирусные средства защиты;

производить мониторинг действий пользователей;

использовать пароли более семи символов.

С уважением,

Руководитель Управления П.Максяков

Козеев С.А.
8 (831) 439-68-75