Приложение № 2

1. Уязвимость встроенного программного обеспечения ПЛК Fastwel (BDU:2025-11171, уровень опасности по CVSS 3.1 – высокий), связанная с переадресацией URL на ненадежный сайт. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, перенаправить пользователя на произвольный URL-адрес.

2. Уязвимость обработчика SSL/TLS микропрограммного обеспечения межсетевых экранов Cisco Adaptive Security Appliance (ASA) и Cisco Firepower Threat Defense (FTD) (BDU:2025-10352, уровень опасности по CVSS 3.1 – высокий), связанная с повторным освобождением памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

3. Уязвимость модуля обнаружения Snort 3 микропрограммного обеспечения межсетевых экранов Cisco Firepower Threat Defense (FTD) (BDU:2025-10353, уровень опасности по CVSS 3.1 – высокий), связанная с выполнением цикла с недоступным условием выхода. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

4. Уязвимость пакетов программ Microsoft Business Productivity Servers, SharePoint Server, SharePoint Enterprise Server и SharePoint Foundation (BDU:2021-01361, уровень опасности по CVSS 3.1 – высокий), связанная с неверным управлением генерацией кода. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

5. Уязвимость веб-инструмента представления данных Grafana (BDU:2023-00493, уровень опасности по CVSS 3.1 – высокий), связанная с неверным ограничением имени пути к каталогу с ограниченным доступом. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, читать произвольные файлы с помощью специально созданного HTTP-запроса.

6. Уязвимость веб-сервера Apache HTTP Server (BDU:2021-04903, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками ограничения имени пути к каталогу. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код или прочитать произвольные файлы в целевой системе.

7. Уязвимость функции __handle_ksmbd_work() в модуле fs/smb/server/server.c внутриядерного CIFS/SMB3-сервера ksmbd server ядра операционной системы Linux (BDU:2025-00153, уровень опасности по CVSS 3.1 – высокий), связанная с повторным использованием ранее освобожденной

памяти. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

8. Уязвимость функции ksmbd_expire_session() в модуле fs/smb/server/mgmt/user_session.c внутриядерного CIFS/SMB3-сервера ksmbd server ядра операционной системы Linux (BDU:2025-00148, уровень опасности по CVSS 3.1 – высокий), связанная с повторным использованием ранее освобожденной памяти. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

9. Уязвимость функции __dst_negative_advice() в модуле include/net/sock.h реализации протокола IPv4 ядра операционной системы Linux (BDU:2024-04585, уровень опасности по CVSS 3.1 – высокий), связанная с повторным использованием ранее освобожденной памяти из-за конкурентного доступа к ресурсу (состояние гонки). Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

10. Уязвимость компонента vfs.c ядра операционной системы Linux (BDU:2025-11865, уровень опасности по CVSS 3.1 – средний), связанная с чтением за допустимыми границами буфера данных. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на целостность данных.

11. Уязвимость функции Preauh_HashValue() компонента ksmbd ядра операционной системы Linux (BDU:2025-10729, уровень опасности по CVSS 3.1 – средний), связанная с ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

12. Уязвимость функции recvmsg() ядра операционной системы Linux (BDU:2025-12988, уровень опасности по CVSS 3.1 – высокий), связанная с копированием буфера без проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

13. Уязвимость компонента ksmbd ядра операционной системы Linux (BDU:2025-12992, уровень опасности по CVSS 3.1 – средний), связанная с неограниченным распределением ресурсов. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

14. Уязвимость драйвера Windows Agere Modem Driver операционных систем Windows (BDU:2025-12990, уровень опасности по CVSS 3.1 – высокий),

связанная с переполнением буфера в стеке. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

15. Уязвимость прошивки SEV-SNP микропрограммного обеспечения графических процессоров AMD (BDU:2025-12991, уровень опасности по CVSS 3.1 – высокий), связанная с ошибками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

16. Уязвимость модуля igel-flash-driver операционных систем IGEL (BDU:2025-12993, уровень опасности по CVSS 3.1 – средний), связанная с ошибками проверки криптографической подписи. Эксплуатация уязвимости может позволить нарушителю обойти существующие ограничения безопасности.

17. Уязвимость функции CryptHmacSign() реализации TCG TPM2 программного стека TPM2 Software Stack (BDU:2025-12994, уровень опасности по CVSS 3.1 – средний), связанная с чтением памяти за пределами выделенного буфера. Эксплуатация уязвимости может позволить нарушителю раскрыть защищаемую информацию.

18. Уязвимость драйвера Agere Modem Driver операционных систем Windows (BDU:2025-12995, уровень опасности по CVSS 3.1 – высокий), связанная с разыменованием недоверенного указателя. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

В целях предотвращения возможности эксплуатации уязвимостей 1–18 рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30 июня 2025 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty) (далее –Методики).

19. Уязвимость диспетчера подключений удаленного доступа (Remote Access Connection Manager) операционных систем Windows (BDU:2025-12964, уровень опасности по CVSS 3.1 – высокий), связанная с ошибками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методиками.

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

минимизировать пользовательские привилегии;

отключить (удалить) неиспользуемые учетные записи пользователей;

использовать системы обнаружения и предотвращения вторжений;

обеспечить использование многофакторной аутентификации (MFA) для RDP-протокола.

20. Уязвимость функции sk_msg_free() файла net/ipv4/af_inet.c ядра операционной системы Linux (BDU:2025-12987, уровень опасности по CVSS 3.1 – средний), связанная с неограниченным распределением ресурсов. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методиками.

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

минимизировать пользовательские привилегии;

отключить (удалить) неиспользуемые учетные записи пользователей;

обеспечить контроль журналов аудита кластера для отслеживания попыток эксплуатации уязвимости.

21. Уязвимость функции recv() компонента tls ядра операционной системы Linux (BDU:2025-12996, уровень опасности по CVSS 3.1 – средний), связанная с недоступным условием выхода. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методиками.

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

минимизировать пользовательские привилегии;

отключить (удалить) неиспользуемые учетные записи пользователей;

обеспечить контроль журналов аудита кластера для отслеживания попыток эксплуатации уязвимости.