Рекомендации по защите систем и сетей, функционирующих под управлением операционных систем Microsoft Windows

1. Минимизировать использование неподдерживаемых версий операционных систем Microsoft Windows (включая устаревшие версии Windows 10). Убедиться, что на всех автоматизированных рабочих местах под управлением Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, где по каким-либо причинам невозможен переход на более новые версии ОС, установлено обновление KB2871997.

2. Убедиться, что на всех доменных автоматизированных рабочих местах для провайдера аутентификации WDigest отключено кеширование паролей интерактивно аутентифицировавшихся пользователей в открытом виде в памяти процесса Lsass. Использовать групповую политику для принудительного отключения данного кеширования, а также реализовать мониторинг изменений отвечающего за данную настройку ключа реестра.

3. Включить на всех доменных автоматизированных рабочих местах принудительную очистку памяти от учётных данных при выходе пользователя из системы путём установки значения ключа реестра, отвечающего за данную настройку.

4. Запретить групповой политикой хранение в штатном менеджере паролей Windows учётных данных для сетевой аутентификации.

5. По возможности использовать на всех доменных автоматизированных рабочих местах механизм LSA Protection для защиты памяти процесса lsass от доступа со стороны недоверенных процессов. Более эффективной альтернативой данному механизму является применение функционала защиты памяти процесса lsass в решениях по защите конечных точек. Например, механизм Credentials Guard, доступный в новых версиях операционных систем Windows.

6. Используя групповую политику, ограничить возможность использования привилегии отладки (SeDebugPrivilege) для административных учётных записей на всех доменных хостах. Если данная привилегия необходима для отдельных категорий пользователей (например, разработчиков), разрешить её только для данных учётных записей.

7. Отключить или ограничить кеширование учётных данных интерактивно вошедших пользователей, используемое для доступа в систему при недоступности контроллеров домена. Для стационарных автоматизированных рабочих мест, имеющих постоянное подключение к системам и сетям, рекомендуется отключить кеширование, для мобильных автоматизированных рабочих мест минимизировать размер кеша до 1-2 записей.

8. Меры защиты информации, направленные на ограничение возможностей нарушителей по использованию полученных учётных данных для перемещения между автоматизированными рабочими местами сети организации.

8.1. Ограничить возможность сетевого доступа между автоматизированными рабочими местами по протоколам DCOM, SMB, RDP. Данное ограничение может быть реализовано с использованием средств межсетевого экранирования, ACL на access-портах коммутаторов, Private VLAN, Wireless Client Isolation.

9. Меры защиты привилегированных учётных записей.

9.1. Использовать усиленные парольные политики для привилегированных учётных записей (более частая смена, повышенные требования к сложности пароля). Для реализации возможности исполнения различных парольных политик для разных категорий пользователей в Windows использовать механизм Fine-Grained Password Policies.

9.2. Для защиты привилегированных учётных записей реализовать многоуровневую модель доступа, подразумевающую выделение как минимум следующих уровней:

Уровень 0: Контроллеры домена;

Уровень 1: Сервера;

Уровень 2: Рабочие станции.

9.3. Для администрирования каждого из уровней должны использоваться раздельные привилегированные учётные записи с применением групповой политики (параметры «Deny access to this computer from the network», «Deny logon locally», «Deny logon through Remote Desktop», «Deny logon as a batch job», «Deny logon as a service») рекомендуется реализовать следующие ограничения:

запрет входа под учётными записями уровня 0 на автоматизированные рабочие места уровней 1 и 2 (запрет входа под доменными администраторами на рабочие станции и сервера);

запрет входа под учётными записями уровня 1 на автоматизированные рабочие места уровней 2 (запрет входа под учётными записями администраторов серверов на рабочие станции).

9.4. Рекомендуется использовать выделенные физические или виртуальные автоматизированные рабочие места для администраторов с усиленными мерами по безопасности, подключенные к изолированному сетевому сегменту.

9.5. Для администрирования автоматизированных рабочих мест использовать штатную учётную запись локального администратора с уникальным паролем на каждой рабочей станции. Обеспечить регулярную смену паролей данных учётных записей, используя механизм LAPS.

9.6. Использовать группу Protected Users для всех привилегированных доменных учётных записей, например, администраторов домена.

9.7. Запретить делегирование для всех привилегированных доменных учётных записей, например, администраторов домена.

9.8. Для безопасного удалённого администрирования операционных систем Windows с использованием RDP рекомендуется принять следующие меры:

исключить возможность доступа по RDP напрямую из сети «Интернет»;

включить обязательную аутентификацию на уровне сети (Network Level Authentication);

настроить автоматическое завершение сессий при отключении от удалённого рабочего стола без завершения сессии;

по возможности использовать Restricted Admin Mode или Windows Defender Remote Credential Guard.

9.9. Обеспечить регулярную (не реже одного раза в год) смену пароля сервисной учётной записи krbtgt. Также необходимо выполнить принудительную внеплановую смену пароля данной учётной записи в следующих ситуациях:

увольнение сотрудника, имевшего привилегии доменного администратора;

подозрение на компрометацию учётной записи с привилегиями доменного администратора.

9.10. Обращаем внимание, что из-за особенностей функционирования среды Active Directory для полной смены пароля krbtgt необходимо поменять его 2 раза подряд.

9.11. Проводить регулярный аудит состава привилегированных групп.

Обращаем внимание, что к привилегированным группам относятся: Domain Admins, Enterprise Admins, Administrators, Schema Admins, Account Operators, Print Operators, Server Operators, Domain Controllers, Read-only Domain Controllers, Enterprise Domain Controllers, Group Policy Creators Owners, DnsAdmins, Key Admins, Organization Management, Exchange Trusted Subsystem, Exchange Windows Permissions.

10. Меры защиты сервисных учётных записей.

10.1. Ограничить количество сервисных учётных записей с разрешённым неограниченным делегированием. По возможности использовать ограниченное делегирование вместо неограниченного.

10.2. Использовать стойкие пароли для сервисных учётных записей и осуществлять их регулярную смену (не реже раза в полгода или квартал). Для автоматизации регулярной смены паролей сервисных учётных записей рекомендуется использовать механизм gMSA. Также необходимо убедиться, что сервисные учётные записи не являются членами привилегированных доменных групп.

10.3. Используя групповые политики, рекомендуется ограничить возможность входа под сервисными учётными записями на автоматизированные рабочие места, где их использование недопустимо (например, интерактивный, RPD или сетевой вход под сервисной учётной записью на пользовательскую рабочую станцию).

10.4. Для администраторов автоматизированных рабочих мест и серверов рекомендуется заводить раздельные учетные записи (с правами обычного пользователя и с повышенными правами). Повседневная деятельность, не требующая повышенных привилегий, должна вестись с правами обычного пользователя.

11. Общесистемные меры защиты информации операционных систем Microsoft Windows.

11.1. Проводить регулярный аудит доменных учётных записей. Особое внимание обращать на следующие учётные записи:

не использовавшиеся длительное время;

длительное время не менявшие пароль;

учётные записи с включенными свойствами «Store password using reversible

encryption», «Password Not Required», «Password Never Expires», «DES Kerberos Encryption Enabled», «Do not require Kerberos Pre-Authentication»;

учётные записи, ассоциированные с людьми (в особенности привилегированные), имеющие прописанные SPN, которые, как правило, указываются только для сервисных учётных записей, либо учётных записей компьютеров.

11.2. Отключить возможность добавления в домен новых автоматизированных рабочих мест непривилегированными пользователями. По умолчанию любой доменный пользователь имеет право на самостоятельное добавление в домен до 10 автоматизированных рабочих мест.

11.3. Включить на всех узлах расширенные политики аудита согласно уровню «Stronger Recommendation».

11.4. Использовать политики «AppLocker» ограничения запуска исполняемых файлов по белому списку.

12. Обеспечить устранения уязвимостей реализации сетевого протокола реализации сетевого протокола SMB операционной системы Windows (BDU:2022-02174, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 - критический), связанной с возможностью перенаправления пользователя на SMB-сервер нарушителя. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код в уязвимой системе.

В целях предотвращения возможности эксплуатации, указанной уязвимости необходимо принять следующие меры:

заблокировать 445 TCP-порт для ограничения возможности обращения к уязвимому компоненту;

использовать средства межсетевого экранирования для формирования «белого» списка приложений и адресов, которым разрешена передача трафика по протоколу SMB;

отключить службу SMB, если она не используется;

сегментировать сеть для блокирования возможностей распространения в системе.

13. Уязвимость сетевой файловой системы Network File System (NFS) операционной системы Windows существует из-за недостаточной проверки входных данных (BDU:2022-02866, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 - критический). Эксплуатация уязвимости позволить нарушителю,

действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо отключить NFSV2 и NFSV3 следующим способом (отключение может негативно повлиять на функционирование системы):

1.Выполнить команду в окне PowerShell:

PS C:\Set-NfsServerConfiguration -EnableNFSV2 $false -EnableNFSV3 $false;

2.Перезапустить сервер NFS или перезагрузить компьютер;

3.Для перезапуска NFS-сервера запустить окно cmd с помощью «Запуск от имени администратора» и ввести следующие команды:

nfsadmin server stop;

nfsadmin server start.

4.Для того, чтобы убедиться, что NFSV2 и NFSV3 отключены, необходимо выполнить команду в окне PowerShell:

PS C:\Set-NfsServerConfiguration.

14. Уязвимость метода интерфейса LSARPC компонента Windows LSA операционной системы Windows (BDU:2022-02882, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 - высокий), связана с возможностью обхода механизма аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, реализовать атаку «человек посередине» путем ретрансляции NTLM на службы сертификатов Active Directory (AD CS).

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо приять меры:

-запретить анонимное подключение в LSARPC;

-включить EPA и отключить HTTP на серверах AD CS;

-включить EPA для веб-службы регистрации сертификатов;

-включить Require SSL с целью использования только HTTPS-соединения;

-отключить NTLM-аутентификации на контроллере домена Windows;

-отключить NTLM на всех серверах AD CS в вашем домене с помощью групповой политики;

-отключить NTLM для информационных служб Интернета (IIS) на серверах AD CS в домене, на которых запущены службы «Веб-регистрация центра сертификации» или «Веб-служба регистрации сертификатов».

15. Уязвимость компонента Kerberos KDC службы каталогов Active Directory операционной системы Windows (BDU:2022-02883, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 - высокий), связана с небезопасным управлением привилегиями. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо использовать механизм ручного сопоставления сертификатов и пользователей путем добавления соответствующей строки сопоставления в атрибут altSecurityIdentities пользователя в Active Directory.

16. Уязвимость утилиты сбора диагностических данных и устранения неполадок Microsoft Support Diagnostics Tool операционных систем Windows (BDU:2022-03226, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – высокий), связанная с ошибками при обработке вызываемого URL-адреса. Эксплуатация уязвимости может позволить нарушителю, действующему удалено, выполнить произвольный код с привилегиями вызывающего приложения. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо принять меры:

1.Отключить протокол обработки URL-адресов, выполнив следующие действия:

-запустить командную строку от имени «Администратора»;

-создать резервную копию раздела реестра путем выполнения команды «reg export HKEY_CLASSES_ROOT\ms-msdt filename»;

-выполнить команду «reg export HKEY_CLASSES_ROOT\ms-msdt /f».

2. Использовать средства антивирусной защиты.

17. Уязвимость сетевой файловой системы Network File System (NFS) операционной системы Windows, существующая из-за недостаточной проверки входных данных (BDU:2022-03517, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический). Эксплуатация данной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо отключить NFS v4.1, выполнив следующие действия:

1) выполнение команды PowerShell:

PS C: \Set-NfsServerConfiguration -EnableNFS V4 $false;

2) перезапуск сервера NFS или перезагрузка компьютера;

3) для проверки отключения NFS v4.1 выполнить команду PowerShell:

PS C: \Get- NfsServerConfiguration.

В результате указанных действий параметр EnableNFS V4.1 должен иметь значение «false».

18. Уязвимость подсистемы Client Server Run-Time Subsystem (CSRSS) операционной системы Windows (BDU:2022-04374, BDU:2022-04375, BDU:2022-04376), связанных с недостатками разграничения доступа. Эксплуатация данной

уязвимости может позволить нарушителю повысить свои привилегии.

В случае невозможности установки обновления операционной системы необходимо принять следующие компенсирующие меры:

-использовать средства антивирусной защиты для детектирования и нейтрализации программ, эксплуатирующих уязвимость;

-использовать механизмы замкнутой программной среды;

-отключить используемые учётные записи, а также учетные записи недоваренных пользователей;

-принудительно сменить пароли пользователей;

-ограничить доступ к командной строке для недоверенных пользователей;

-осуществить мониторинг действий пользователей.

19. Уязвимость почтового сервера Microsoft Exchange Server (BDU:2022-06032, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), связанная с ошибками управления генерации кода. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код и аутентифицировать доступ к уязвимому серверу.

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

1.открыть диспетчер IIS. Для этого необходимо открыть Панель управления (Control Panel), далее программы и компоненты (Programs and Features), далее Включение или отключение компонентов Windows (Turn Windows Features on or off) и развернуть узел Службы IIS.

2.развернуть веб-сайт по умолчанию.

3.выбрать «Автообнаружение».

4.в представлении функций нажать «Перезаписать URL».

5.на панели «Действия» справа нажать «Добавить правила».

6.выбрать «Блокировка запроса» и нажать «ОК».

7.вывести следующую команду:

.**autodiscover.\json. *\@. *Powershell.** и нажать «ОК».

8.развернуть правило и выбрать правило с шаблоном .**autodiscover.\json. *\@. *Powershell.** и нажать «Изменить» в разделе «Условия».

-изменить ввод условия с {URL} на {REQUEST_URI};

-блокировать HTTP-портов 5985 и 5986.

20. Уязвимость почтового сервера Microsoft Exchange Server (BDU:2022-06064, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанной с ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно,

проводить спуфинг-атаки.

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

-использовать средства антивирусной защиты с функцией контроля доступа к веб-ресурсам;

-реализовать контролируемый доступ в сеть Интернет – регламентацию разрешенных сетевых ресурсов и соединений;

-осуществлять запуск веб-браузера от имени пользователя с минимальными возможными привилегиями в операционной системе;

-использовать иные веб-браузера;

-применять системы обнаружения и предотвращения вторжений.

21. Уязвимость механизма Mark-of-the-Web (MoTW) операционных систем Windows (BDU:2022-06491, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), связанная с возможностью запуска произвольных JavaScript-файлов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти механизмы безопасности и выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

-использовать средства антивирусной защиты;

-использовать изолированную программную среду для работы с файлами из недоверенных источников.

22. Уязвимость реализации протокола Kerberos операционных систем Windows (BDU:2022-02861, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с возможностью запуска произвольных JavaScript-файлов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти механизмы безопасности и выполнить произвольный код.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие 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».

23. Уязвимость утилиты ntfs-3g набора драйверов NTFS-3G реализации файловой системы NTFS (BDU:2022-06607, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – высокий), связанная с ошибками при обработке

метаданных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти механизмы безопасности и выполнить произвольный код.

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

-отключить возможность автоматического монтирования NTFS-разделов;

-ограничить возможность подключения недоверенных USB-устройств.

23. Уязвимость функционала проверки сертификата X.509 библиотеки OpenSSL (BDU:2022-06609, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – высокий), связанная с ошибками при обработке метаданных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти механизмы безопасности и выполнить произвольный код.

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

24. Уязвимость функционала проверки сертификата X.509 библиотеки OpenSSL (BDU:2022-06609, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с переполнением буфера в стеке. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, аварийно завершить работу приложения.

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

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

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

-отлучить 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.

26. Уязвимость операционной системы Windows (BDU:2023-00065, уровень опасности по CVSS 3.0 – высокий), связанная с ошибками при обработке вызовов Advanced Local Process Call (ALPC). Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии и выполнить произвольный код с привилегиями SYSTEM.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

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

- использовать антивирусные средства защиты;

-использовать замкнутую программную среду;

-осуществить минимизацию пользовательских привилегий;

-производить мониторинг действий пользователей;

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

-осуществить принудительную смену паролей пользователей.

27. Уязвимость службы резервного копирования Windows Backup Service операционных систем Windows (BDU:2023-00067, уровень опасности по CVSS 3.0 – средний), связанная с ошибками при управлении привилегиями. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии до уровня SYSTEM.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

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

- использовать антивирусные средства защиты;

-использовать замкнутую программную среду;

-осуществить минимизацию пользовательских привилегий;

-производить мониторинг действий пользователей;

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

-осуществить принудительную смену паролей пользователей.

28. Уязвимость драйвера файловой системы журнала операционных систем Windows (BDU:202-06934, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – высокий), связанной с записью за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код с системными привилегиями.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

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

- использовать антивирусные средства защиты для детектирования и нейтрализации программ, эксплуатирующих уязвимость;

-ограничить доступ к устройствам из корпоративной и интернет-сети с использованием сертифицированных межсетевых экранов и систем обнаружения вторжений;

-использовать многофакторную аутентификацию для удаленного доступа.