

Table of Contents

Table of Contents	1
Безопасность	2
Интерпретация результатов сканирования	3
53(UDP)-DNS Отказ в обслуживании.	4
DNS-сервер поддерживает рекурсию запросов.	5
443(TCP) - HTTP SSL	6
Слабый криптографический ключ	7
623(UDP) - IPMI	8
Обнаружение уязвимости типа CVE-2002-20001 при сканировании NGFW UserGate сторонними сканерами.	9
Статус портов при сканировании Nmap	10
Сканирование сети обнаруживает порты даже на тех адресах, где нет соответствующих сервисов	11
Ложные срабатывания сигнатур IDS	12

Интерпретация результатов сканирования

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn, UserGate SIEM

Очень часто нам задают вопросы по уязвимостям обнаруженным сторонними сканнерами безопасности в наших продуктах. Ниже представлены ответы на подобные вопросы.

53(UDP)-DNS Отказ в обслуживании.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Версия сервера: Usergate DNS v7.0.1.989R

Высокий уровень

Отказ в обслуживании

ID: 8352

CVE: CVE-2016-2776

Дата публикации: 27.09.2016

Краткое описание:

Уязвимость позволяет злоумышленнику вызвать отказ в обслуживании (ошибку утверждения и завершение работы демона).

Описание

Уязвимость в buffer.c в named в ISC BIND, связанная с некорректным построением ответов, позволяет злоумышленникам, действующим удаленно, вызвать отказ в обслуживании (ошибку утверждения и завершение работы демона) при помощи специально сформированного запроса.

Ответ

В продукте UserGate в качестве DNS сервера **не используются** версии компонента ISC BIND, подверженные данной уязвимости.

DNS-сервер поддерживает рекурсию запросов.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Уязвимость: Рекурсия

ID: 1058

CVE: CVE-1999-0024

Дата публикации: 13.08.1997

Описание:

DNS-сервер поддерживает рекурсию запросов. При определенных обстоятельствах злоумышленник может вызвать на сервере отказ в обслуживании.

Ответ

В продукте UserGate ограничена глубина рекурсии DNS запросов, в связи с этим вызвать отказ в обслуживании данным способом не представляется возможным, данная уязвимость не применима к продукту UserGate.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Уязвимость: Некорректная цепочка сертификатов

ID: 7034

Описание:

При проверке цепочки доверия сертификата данного сервиса были обнаружены следующие ошибки # Цепочка сертификатов не полная

Ответ

В продукте UserGate используются самоподписанные сертификаты. Поскольку сертификаты не подписаны каким-либо удостоверяющим центром, сканеры определяют цепочку с их участием неполной. Для устранения данной уязвимости необходимо заменить сертификат по умолчанию на подписанный удостоверяющим центром пользовательский сертификат.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Уязвимость:

Слабый криптографический ключ

ID: 8309

Краткое описание:

Обнаружен слабый криптографический ключ. Длина ключа, используемая криптографическим алгоритмом, определяет уровень безопасности, который может быть достигнут.

Алгоритм (длина ключа): rsaEncryption(1024)

Ответ

В продукте UserGate используются сертификаты по умолчанию (default) с длиной ключа 1024. Для устранения данной уязвимости необходимо заменить сертификат по умолчанию (default) на пользовательский сертификат с требуемой длиной ключа.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Уязвимость:

Найден логин и хэш пароля пользователя IPMI

ID: 8312

CVE: CVE-2013-4786

Краткое описание:

Был подобран логин и получен SHA-1 хэш пароля учетной записи IPMI. Если пароль недостаточно сложный, его можно восстановить с помощью общедоступных утилит.

Ответ

Функционал модуля IPMI опционален, требуется только для подключения из локальной сети организации. Не рекомендуется публиковать доступ к данному интерфейсу во внешнюю сеть, где существуют риски эксплуатации данной уязвимости.

Version: 6.x, 7.x

Product: UserGate NGFW

Задача

Сканирование NGFW UserGate сторонними сканерами показывает открытую уязвимость типа CVE-2002-20001 Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater). Как устранить?

Решение

Уязвимость CVE-2002-20001 Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) использует механизм реализации протокола обмена ключами Diffie-Hellman Key Exchange (DHE). Злоумышленник со стороны клиента может отправлять на сервер произвольную последовательность под видом открытого ключа, вызывая повышение загрузки CPU сервера вычислениями протокола DHE. Согласно методике оценки уязвимостей (CVSS) она имеет высокую, но не критичную оценку (7.5) и влияет на доступность ресурса, при этом конфиденциальность данных и целостность ресурса не находятся под угрозой. Эффективность потенциальной атаки с использованием этой уязвимости во многом зависит от типа используемого криптографического протокола, конкретной реализации системной библиотеки, а также размера ключа, используемого во время обмена ключами. В базовом сценарии атаки клиент запрашивает использование только протокола DHE и максимально возможную длину ключа.

В решениях UserGate используется протокол DHE. Анализ воздействия уязвимости на конкретную реализацию DHE в оборудовании UserGate не показал ее влияния на производительность. В качестве дополнительных мер безопасности можно сделать следующее:

- Отключить протокол DHE в настройках используемых [профилей SSL](#) для удаленного доступа к устройству. Вместо DHE могут использоваться протоколы RSA (для поддержки устаревших приложений) и/или ECDHE.
- Ограничить количество и тип DH групп в настройках [профилей безопасности VPN](#) только реально используемыми.

Technology: Firewall

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Что означают статусы портов при сканировании nmap или им подобным.

Ответ

Nmap и ему подобные сканеры портов определяют 6 состояний программного порта:

Открыт (open)

Приложение принимает запросы на TCP соединение или UDP пакеты на этот порт.

Закрыт (closed)

Закрытый порт доступен (он принимает и отвечает на запросы Nmap), но не используется каким-либо приложением.

Фильтруется (filtered)

Администраторы могут заблокировать порты с помощью брандмауэров. в этом случае Nmap не может определить, открыт ли порт, т.к. фильтрация пакетов не позволяет достичь запросам Nmap этого порта.

Не фильтруется (unfiltered)

Это состояние означает, что порт доступен, но Nmap не может определить открыт он или закрыт.

Открыт|фильтруется (open|filtered)

Nmap характеризует порт таким состоянием, когда не может определить открыт порт или фильтруется. Это состояние возникает при таких типах сканирования, при которых открытые порты не отвечают. Отсутствие ответа также может означать, что пакетный фильтр не пропустил запрос или ответ не был получен. Поэтому Nmap не может определить наверняка открыт порт или фильтруется. При сканировании UDP, по IP протоколу, FIN, NULL, а также Xmas порт может быть охарактеризован таким состоянием.

Закрыт|фильтруется (closed|filtered)

Это состояние используется, когда Nmap не может определить закрыт порт или фильтруется.

Technology: Firewall

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Задача

При сканировании IP адресов серверов, защищенных UserGate NGFW, порты, на которых нет соответствующих сервисов, показываются в статусе "закрытый".

Решение

Сканеры типа Nmap распознают [статус](#) порта по ответу от сканируемого ресурса. Статус "закрыт" означает, что на отправку сканером пакета SYN, цель ответила пакетом RST. Это означает, что данный порт доступен, но на нем не запущено никаких сетевых сервисов. Если этот порт разрешен на межсетевом экране UserGate NGFW, это нормальное поведение системы. В противном случае следует внимательно изучить настройки межсетевого экрана UserGate NGFW и устранить ошибки конфигурирования.

Если есть список устройств, для которых необходимо сделать порт недоступным, то можно создать правило DNAT в неиспользуемый адрес и заблокировать трафик на этот адрес правилом межсетевого экрана.

Product: UserGate NGFW

Version: 6.x, 7.x

Задача

Происходят ложные срабатывания сигнатур COB

Решение

Чтобы исключить ложные срабатывания:

1. Создать профиль COB.

Перейдите в раздел **Библиотеки → Профили COB**. На панели **Профили** нажмите **Добавить** и создайте профиль COB. Выбрав профиль нажмите **Добавить** на панели **Сигнатуры**. Далее укажите сигнатуры, ложные срабатывания которых нужно исключить.

2. Исключить срабатывание сигнатуры.

После создания профиля COB с необходимым набором сигнатур перейдите в раздел **Политики безопасности → COB**. Откройте настройки правила, действие которого выполнится в результате срабатывания сигнатуры (правила с действиями **Журналировать** или **Запретить**); во вкладке **Профили исключения** добавьте профиль COB с сигнатурами, создающими ложные срабатывания.

Подробнее о настройке системы обнаружения и предотвращения вторжений читайте в [UserGate 6. Руководство администратора](#).

