ФСТЭК РОССИИ
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПО ДАЛЬНЕВОСТОЧНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
Ленина, д. 37, г. Хабаровск, 680030
Тел., факс (4212) 35-11-08
E-mail: dfo@fstec.ru

22.06.2022 г. № 2/3750

На № _____

Первому вице-губернатору
Хабаровского края,
председателю Совета по
информационной безопасности
при Губернаторе Хабаровского края
А.А.НИКИТИНУ

main@adm.khv.ru

О мерах по повышению защищенности информационной инфраструктуры Российской Федерации

Уважаемый Александр 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, просим обратить внимание на необходимость устранения следующих уязвимостей:

1. Уязвимость веб-интерфейса управления микропрограммного обеспечения маршрутизаторов Cisco Small Business RV 110W, RV 130, RV 130W и RV 215W, связанная с недостаточной проверкой вводимых данных (BDU:2022-03519, уровень опасности по CVSS 2.0 — критический уровень опасности, по CVSS 3.0 — критический уровень опасности). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код или вызвать отказ в обслуживании путем отправки специально сформированных HTTP-пакетов.

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

выделение веб-интерфейса управления в отдельный сегмент сети с ограничением доступа к нему средствами межсетевого экранирования;

исключение доступа к веб-интерфейсу управления из общедоступных сетей (Интернет);

использование межсетевого экрана уровня приложений;

использование системы обнаружения и предотвращения вторжений.

2. Уязвимость функции внешней аутентификации устройства управления защитой контента Cisco Secure Email and Web Manager (ранее Cisco Security Management Appliance и Cisco Email Security Appliance), связанная с ошибками разграничения доступа (BDU:2022-03520, уровень опасности по CVSS 2.0 — критический уровень опасности, по CVSS 3.0 — критический уровень опасности). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к веб-интерфейсу устройства.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо отключить функцию «Внешняя аутентификация» в веб-интерфейсе устройства.

3. 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 уровень опасности, по CVSS 3.0 — критический уровень опасности). Эксплуатация 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-NfsServerCon figuration -EnableNFSV4 $false;

2) перезапуск сервера NFS или перезагрузка компьютера;

3) для проверки отключения NFSv4.1 выполнить команду PowerShell:

PS C:\Get-NfsServerConfiguration.

В результате указанных действий параметр EnableNFSv4.1 должен иметь значение «False».

С уважением,

Исполняющий обязанности
руководителя Управления Р.Хабибулин