

Множественные уязвимости в Cisco IOS

Программа: Cisco IOS 12.x.

Опасность: Средняя.

Описание: 1. Уязвимости обнаружены из-за ошибок в функционале Data-link Switching (DLSw). Удаленный пользователь может с помощью специально сформированных UDP-или IP Protocol 91-пакетов вызвать утечку памяти или перезагрузить уязвимое устройство.

2. Уязвимость существует из-за ошибки в реализации Multicast Virtual Private Network (MVPN). Удаленный пользователь может с помощью специально сформированного сообщения создать дополнительные групповые состояния на базовых маршрутизаторах и получить групповой трафик от других VPN-сетей, основанных на Multiprotocol Label Switching (MPLS).

3. Уязвимость существует из-за неизвестной ошибки на устройствах Cisco Catalyst 6500 Series и Cisco 7600 Router с Cisco IOS 12.2, которая позволяет удаленному пользователю предотвратить прохождение трафика по уязвимому интерфейсу. Для успешной эксплуатации уязвимости устройство должно быть сконфигурировано для Open Shortest Path First (OSPF) Sham-Link и Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). Уязвимости подвержены только устройства Cisco Catalyst 6500 Series и Catalyst 7600 Series с модулями Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) и Route Switch Processor 720 (RSP720). Потенциально уязвимыми являются Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C и Route Switch Processor 720-3CXL.

4. Уязвимость существует из-за неизвестной ошибки при обработке UDP-пакетов. Удаленный пользователь может с помощью специально сформированного UDP-пакета, отправленного на IPv6-интерфейс определенной службе (слушающей также и на IPv4-интерфейсе), аварийно завершить работу интерфейса или, в случае со службой RSVP (Resource Reservation Protocol), аварийно завершить работу устройства.

5. Две уязвимости обнаружены в функционале virtual private dial-up network (VPDN), когда используется PPTP-протокол. Удаленный пользователь может вызвать утечку памяти и аварийно завершить работу PPTP-сессии или заставить устройство потратить все доступные блоки дескрипторов и вызвать отказ в обслуживании устройства.

URL производителя: www.cisco.com.

Решение: Установите исправление с сайта производителя.

Целочисленное переполнение в FreeBSD

Программа: FreeBSD 6.x и 7.0.

Опасность: Низкая.

Описание: Множественные целочисленные переполнения обнаружены в функции strfmon() в библиотеке libc. Удаленный пользователь может с помощью специально сформированной форматной строки аварийно завершить работу приложения или выполнить произвольный код на системе.

URL производителя: www.freebsd.org.

Решение: В настоящее время способов устранения уязвимости не существует.

Переполнение буфера в Novell eDirectory

Программа: Novell eDirectory 8.8.1 и, возможно, более ранние версии; Novell eDirectory 8.7.3.9 и, возможно, более ранние версии.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки проверки границ данных при обработке LDAP Extended Request-сообщений в библиотеке libldap. Удаленный пользователь может с помощью слишком большого LDAP delRequest-сообщения вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.novell.com/products/edirectory.

Решение: Установите последнюю версию 8.8.2 или установите исправление eDirectory 8.7.3 sp10 с сайта производителя.

Выполнение произвольных команд в Sun Solaris

Программа: Sun Solaris 10.

Опасность: Средняя.

Описание: Уязвимость существует из-за некорректной обработки имен карт, отправленных с помощью обновления демону gpc.upupdated. Удаленный пользователь может с помощью специально сформированного имени карты выполнить произвольные команды на системе. Для успешной эксплуатации уязвимости демон gpc.upupdated должен быть запущен с опцией «-i» (не используется по умолчанию).

URL производителя: www.sun.com.

Решение: В настоящее время способов устранения уязвимости не существует.

Уязвимость при обработке пакетов в SILC Server

Программа: SILC Secure Internet Live Conferencing Server версии до 1.1.1.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки при обработке NEW_CLIENT-пакетов. Удаленный пользователь может с помощью NEW_CLIENT-пакета, не содержащего имени пользователя, аварийно завершить работу приложения.

URL производителя: silcnet.org/software/download/server.

Решение: Установите последнюю версию 1.1.1 с сайта производителя.

Обход ограничений безопасности в OpenSSH

Программа: OpenSSH версии до 4.9 и 4.9p1.

Опасность: Низкая.

Описание: Уязвимость существует из-за некорректной реализации директивы «ForceCommand». Локальный пользователь может выполнить произвольные команды на системе с помощью файла ~/.ssh/rc, даже если включена директива «ForceCommand».

URL производителя: openssh.com.

Решение: Установите последнюю версию 4.9 или 4.9p1 с сайта производителя.

Составил Александр Антипов