

Несколько уязвимостей в IBM Lotus Domino Web Server

Программа: IBM Lotus Domino версии до 7.0.3 Fix Pack 1 (FP1) и 8.0.1.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за недостаточной обработки входных данных в сервлете веб-контейнера. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасного уязвимого сайта.

2. Уязвимость существует из-за ошибки проверки границ данных в Lotus Domino Web Server. Удаленный пользователь может с помощью слишком длинного HTTP-заголовка Accept-Language вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.lotus.com/products/product4.nsf/wdocs/dominohomepage.

Решение: Установите последнюю версию 7.0.3 Fix Pack 1 (FP1) или 8.0.1 с сайта производителя.

Переполнение буфера в CA Secure Content Manager

Программа: CA eTrust Content Manager 8.0.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных в службе HTTP Gateway (ichttp.exe on port 8080/TCP) при обработке определенных FTP-команд. Удаленный пользователь может с помощью слишком длинного ответа для команд LIST и PASV вызвать переполнение стека и выполнить произвольный код на целевой системе с привилегиями учетной записи SYSTEM.

2. Уязвимость существует из-за ошибки проверки границ данных в службе HTTP Gateway (ichttp.exe on port 8080/TCP) во время преобразования списка FTP-директорий и файлов в HTML. Удаленный пользователь может с помощью слишком длинной строки вызвать переполнение стека и выполнить произвольный код на целевой системе с привилегиями учетной записи SYSTEM.

URL производителя: www3.ca.com/Solutions/Product.asp?ID=4673.

Решение: Установите исправление с сайта производителя.

Целочисленное переполнение в OpenOffice

Программа: OpenOffice 2.4 и более ранние версии.

Опасность: Высокая.

Описание: Целочисленное переполнение обнаружено в функции `rtl_allocateMemory()`. Удаленный пользователь может с помощью специально сформированного документа вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.openoffice.org.

Решение: Установите последнюю версию 2.4.1 с сайта производителя.

Переполнение буфера в Evolution

Программа: GNOME Evolution 2.22.1, возможно, более ранние версии; Novell Evolution 2.22.1, возможно, более ранние версии.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных при обработке строк временной зоны, содержащихся во вложениях iCalendar. Удаленный пользователь может с помощью слишком длинной строки вызвать переполнение статического буфера и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости плагин iTip Formatter должен быть отключен.

2. Уязвимость существует из-за ошибки проверки границ данных при ответе на запрос iCalendar при включенном виде календаря. Удаленный пользователь может внедрить слишком длинное свойство DESCRIPTION во вложение iCalendar, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости пользователь должен принять запросы iCalendar и ответить на них из окна Calendars.

URL производителя: www.novell.com/products/desktop/features/evolution.html.

Решение: В настоящее время способов устранения уязвимости не существует. Некоторые производители Linux-систем выпустили исправления.

Множественные уязвимости в Black Ice Barcode SDK

Программа: Black Ice Barcode SDK 5.01, возможно, более ранние версии.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за использования небезопасного метода `DownloadImageFileURL()` в BIDIB.BIDIBCtrl.1 ActiveX (BIDIB.ocx)-компоненте. Удаленный пользователь может с помощью специально сформированного веб-сайта загрузить злонамеренный файл в произвольную директорию на системе.

2. Уязвимость существует из-за ошибки в BIDIB.BIDIBCtrl.1 ActiveX-компоненте при обработке метода «`DownloadImageFileURL()`». Удаленный пользователь может с помощью специально сформированного веб-сайта передать уязвимому методу слишком длинные аргументы, вызвать повреждение памяти и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки проверки границ данных в BITIFF.BITiffCtrl.1 ActiveX (BITiff.ocx)-компоненте при обработке аргументов в методе `SetByteOrder()`. Удаленный пользователь может с помощью специально сформированного веб-сайта передать слишком длинные аргументы уязвимому методу, вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.blackice.com/barcode.htm.

Решение: В настоящее время способов устранения уязвимости не существует.

Составил Александр Антипов