Автор: Administrator
14.12.2015 10:18

{jcomments on}

***Бреши позволяют удаленному пользователю выполнить произвольный код и раскрыть важные данные.***

Пользователь ресурса Google Code обнаружил четыре уязвимости в антивирусе Avast. Двум брешам, позволяющим выполнить произвольный код, был присвоен статус критических.

Первая из описанных уязвимостей позволяет выйти за пределы памяти в Avast Server Edition. Брешь позволяет удаленному пользователю расшифровать и запустить исполняемые файлы, зашифрованные с помощью PEncrypt. Бреши присвоен статус критической.

Вторая уязвимость позволяет переполнить динамическую память в компоненте AvastSvc.exe. Исследователь смог проэксплуатировать брешь с помощью зашифрованного и упакованного в архив MoleBox изображения. Уязвимость позволяет выполнить удаленный код.

Исследователь безопасности также обнаружил две менее опасные уязвимости. Одна брешь позволяет вызвать целочисленное переполнение с помощью специально

сформированного файла TTC. Вторая уязвимость позволяет раскрыть важные данные с помощью файла базы данных Microsoft Access.

В настоящее время производитель устранил обнаруженные уязвимости. К сожалению, на Google Code не указано, какие именно версии антивируса Avast могут быть уязвимы.

Источник: www.securitylab.ru