АНАЛИЗ ОПАСНОСТИ ГРУПП ЭКСПЛОЙТОВ

Поддубный В.О.
Научный руководитель – к.т.н, доц. Федюшин А.И.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Безопасности информационных технологий, тел. (097) 232-81-66)
e-mail: vadym.poddubnyi@nure.ua

When creating software , it is impossible not to make mistakes, sometimes they can be almost useless, but some can be used to attack the software or the system. An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware. Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack. The aim of the work was to determine the most dangerous exploits group. The result of the work shows that at this point in time browser exploits are the most dangerous and require further study and work with them.

На этапе конфигурирования и настройки автоматизированной системы (АС) требуется проверить, правильно ли подобраны и настроены средства защиты информации, выбрана ли верная политика безопасности. Во время эксплуатации системы также следует регулярно осуществлять аудит безопасности, так как любая система со временем меняется, добавляются новые компоненты, и, следовательно, появляются новые угрозы. Но даже при выполнении всех норм безопасности нельзя гарантировать, что АС будет защищена от атак с использованием эксплойтов, так как ошибки на этапе создания и эксплуатации программного обеспечения (ПО) очень трудно предугадать. Каждый день появляются сотни новых эксплойтов для различных приложений операционных систем (ОС), и несмотря на своевременное обновление баз сигнатур антивирусов и средств защиты, атаки наносят колоссальный урон. Количество веб-сайтов и спам-рассылок с эксплойтами увеличивается. Так, число атак, совершенных с помощью эксплойтов, в 2016 году выросло по сравнению с 2015–м практически на четверть. А корпоративных клиентов, подвергшихся подобным нападениям, за тот же период оказалось больше на 28% – их количество выросло с 538 тысяч до 690 тысяч.

За период 12.02.19–19.02.19 было обнаружено 482 новых уязвимостей из них 37% высокой степени угрозы, 11,5%средней, 51,5% низкой. Из них 5,4% не были исправлены [1].

Эксплойты фактически предназначены для выполнения сторонних действий на уязвимой системе и могут быть разделены между собой следующим образом:

1) Эксплойты для операционных систем;

2) Эксплойты для прикладного ПО (музыкальные проигрыватели, офисные пакеты и т. д.);

3) Эксплойты для браузеров (Internet Explorer, Mozilla Firefox, Opera и другие);

4) Эксплойты для интернет-сайтов (facebook.com, hi5.com, livejournal.com);

5) Эксплойты для интернет-продуктов (IPB, WordPress, VBulletin, phpBB);

6) Другие эксплойты.

Оценивать будем только первые 4 группы, поскольку они имеют наибольшее распространение.

Для определения опасности группы эксплойтов будем брать совокупную оценку исходя из опасности эксплойта и оценки CVSSv2.

Общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS) – это система, позволяющая осуществлять сравнение уязвимостей ПО с точки зрения их опасности. При выставлении оценки используются базовые, временные и контекстные метрики.

Существует 4 вида эксплойтов по степени опасности это низкая, средняя, высокая, критическая.

Максимальная оценка опасности –20 (в случае если все уязвимости критические), минимальная 0. Распределение угроз: 0-5– малая степень угрозы, 5-10, – средняя, 10-15 –. высокая, 15-20 – критическая.

В работе исходя из критериев оценки уязвимостей промышленного стандарта CVSSv2, а также дополнительных контекстных метрик был проведен сравнительный анализ опасности групп эксплойтов и получены статистические оценки. Результаты свидетельствуют, что наиболее опасная группа эксплойтов это эксплойты для браузеров: общий коэффициент опасности – 9,78 по сравнению с 5,42 – для ОС, 7,31 – для прикладного ПО и 3,05 – для сайтов. Таким образом, можно сделать вывод, что эксплойты для браузеров обладают предпороговой с высокой средней угрозой, для ОС и ПО средней угрозой, для сайтов низкой.

Браузерные эксплойты являются довольно распространенным явлением, они могут получать информацию пользователя и использовать ресурсы компьютера. Основная угроза, это угроза конфиденциальности, так как браузер хранит файлы cookies, историю посещений, пароли к сайтам и т.п., которые могут быть похищены и использованы злоумышленником. Дыры в защите существуют у таких браузеров как Microsoft Edge, Mozilla Firefox, Google Chrome, регулярное их обновление и применение защитных мер способны улучшить ситуацию.

Список источников:

1 База данных уязвимостей.– Режим доступа: URL: https://www.cybersecurity-help.cz/vdb/– 19.02.2019г. — Загл. с экрана.