УЯЗВИМОСТЬ ПЕРЕПОЛНЕНИЯ СТЕКА ДЛЯ ИСПОЛНЕНИЯ ВРЕДОНОСНОГО КОДА

А.В. Волощик

Речь пойдет о стеке вызовов. Если кратко, то в нем есть переданные в функцию переменные (аргументы), локальные переменные и адрес возврата. Переполнение стека может привести к его контролю со стороны злоумышленника. А это может повлечь как модификацию локальных переменных в функции, так и подмену ее адреса возврата на вредоносный код. Притом уязвимость может работать и на современных ОС.

В рамках данной работы раскрыта тема использования уязвимости переполнения стека, показана возможность исполнения вредоносного кода. Необходимо отметить, что уязвимость не является распространенной на данный момент, вследствие наличия встроенной защиты в современных высокоуровневых языках программирования. Низкоуровневые языки слабо защищены от этой уязвимости, т. к. позволяют прямо обращаться к памяти. Однако актуальные версии компиляторов (C и C++) предусматривают механизмы защиты и предупреждения, такие как warnings о небезопасных функциях (вроде strcpy, gets), stack canary (дополнительная область стека, перезапись значения которой вызывает срабатывание защиты) и многие другие со стороны самой ОС.

Проанализировав ресурсы OWASP и CWE, исходные коды некоторых продуктов на GitHub (Facebook, Microsoft и др.) можно сказать, что проблема отслеживается указанными компаниями, но в компаниях, которые не выделяют бюджет под InfoSec отделы (мелкий и средний бизнес) могут существовать подобные уязвимости [1–3].

Литература

1. Protostar: Andrew Griffiths&; Exploit Education [Electronic resource]. – Access mode: exploit.education/protostar. – Date of access: 07.05.2021.

2. Exploit Database – Exploits for Penetration Testers, Researchers, and Ethical Hackers [Electronic resource]. – Access mode: www.exploit-db.com. – Date of access: 07.05.2021.

3. Smashing The Stack For Fun And Profit [Electronic resource]. – Access mode: www-inst.eecs.berkeley.edu//~cs161/fa08/papers/stack_smashing.pdf. – Date of access: 07.05.2021.