УДК 004

Вязников Никита Андреевич
студент кафедры защищённых систем связи
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Селиванова Татьяна Евгеньевна
ассистент кафедры защищённых систем связи
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

УСТОЙЧИВОСТЬ ОПЕРАЦИОННОЙ СИСТЕМЫ ASTRA LINUX К РАСПРЕДЕЛЕННЫМ АТАКАМ ТИПА UDP-FLOOD В КОНФИГУРАЦИИ ПО УМОЛЧАНИЮ

Аннотация: В статье проводится детальный теоретический и практический анализ устойчивости отечественной операционной системы Astra Linux при воздействии деструктивного сетевого трафика типа UDP-flood. Исследуются системные аспекты функционирования сетевого стека ядра, включая механизмы программных прерываний, ksoftirqd, и распределения ресурсов сетевых интерфейсов. Рассматриваются особенности генерации диагностических сообщений ICMP и состояние стандартных механизмов сетевой фильтрации. На основе результатов имитационного моделирования определяются критические точки деградации производительности сетевого стека. Сформулированы научно обоснованные практические рекомендации по модификации системных параметров ядра и внедрению механизмов ранней фильтрации пакетов для минимизации рисков отказа в обслуживании.

Ключевые слова. операционная система Astra Linux, информационная безопасность, сетевой стек ядра, атака типа UDP-flood, программные прерывания ksoftirqd, ограничение трафика, сетевой экран ufw.

Vyaznikov Nikita Andreevich,
student of the Department of Secure Communication Systems,
Saint Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich.
Selivanova Tatyana Evgenievna,
assistant at the Department of Secure Communication Systems,
Saint Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich.

THE STABILITY OF THE ASTRA LINUX OPERATING SYSTEM TO DISTRIBUTED ATTACKS SUCH AS UDP FLOOD IN THE DEFAULT CONFIGURATION

Abstract: The article provides a detailed theoretical and practical analysis of the stability of the domestic Astra Linux operating system under the influence of destructive network traffic such as UDP flood. The system aspects of the functioning of the kernel network stack are investigated, including the mechanisms of software interrupts, ksoftirqd, and resource allocation of network interfaces. The features of ICMP diagnostic message generation and the status of standard network filtering mechanisms are considered. Based on the simulation results, critical degradation points of the network stack performance are determined. Scientifically based practical recommendations have been formulated for modifying the system parameters of the kernel and introducing early packet filtering mechanisms to minimize the risks of denial of service.

Keywords. Astra Linux operating system, information security, kernel network stack, UDP flood attack, ksoftirqd software interrupts, traffic restriction, ufw firewall.

Настоящее исследование направлено на оценку способности операционной системы Astra Linux противостоять деструктивным воздействиям типа UDP-flood при использовании стандартных параметров функционирования. Настоящее исследование направлено на оценку устойчивости Astra Linux к атакам типа UDP-flood в базовой конфигурации для выявления системных узких мест и формирования методов повышения защищенности

Архитектурные основы обработки сетевого трафика в ядре Linux

Поступление пакета на сетевую карту и его прохождение через сетевой стек до принятия решения о сбросе создает значительные накладные расходы на выполнение инструкций ядра, что подтверждается результатами эксперимента.

$$PPS = \frac{C_{link}}{8 \times (L_{packet} + L_{overhead})}$$

Обработка пакетов, направленных на закрытые порты, принуждает ядро генерировать ICMP-ответы, что создает критическую нагрузку на процессор [1].

Если входящий датаграммный пакет адресован на закрытый порт, ядро операционной системы выполняет поиск соответствующего открытого сокета в глобальной хэш-таблице. При отсутствии процесса, ожидающего данные на указанном порту, ядро инициирует процедуру генерации и отправки исходящего диагностического сообщения об ошибке протокола межсетевых управляющих сообщений с кодом недоступности порта. Данная процедура требует дополнительных вычислительных затрат на создание новой структуры буфера сокета, заполнение заголовков, расчет контрольных сумм и маршрутизацию исходящего сообщения, что превращает обработку каждого мусорного пакета в ресурсоемкую операцию. В Astra Linux межсетевой экран UFW по умолчанию неактивен, а настройки ядра (sysctl) ориентированы на совместимость, а не на

фильтрацию трафика [2].

Устойчивость Astra Linux SE к UDP-flood оценивалась на изолированном стенде с использованием генератора трафика hping3.

Таблица 1. Влияние интенсивности сетевой атаки на показатели производительности

Плотность атаки, Мбит/с	**Загрузка процессора потоками, %**	**Коэффициент потери легитимных пакетов, %**	**Задержка сетевых ответов ICMP, мс**
0	0.2	0.0	0.7
10	19.4	1.1	5.2
30	48.1	7.9	14.8
50	81.3	25.6	52.1
100	100.0	98.2	874.5

Источник: анализ автора

Данные таблицы 1 демонстрируют, что при интенсивности атаки 50 Мбит/с загрузка CPU превышает 80%, а при 100 Мбит/с система теряет 98% легитимного трафика, что является состоянием отказа в обслуживании.

Научно обоснованные методы повышения устойчивости системы

Для минимизации последствий UDP-flood и повышения устойчивости Astra Linux предлагается трехуровневая модель защиты, базирующаяся на фильтрации на разных этапах прохождения трафика [3].

Первый уровень защиты заключается в активации встроенного брандмауэра ufw и переходе от глобальных ограничений лимитов к динамическому поадресному контролю. Использование модуля hashlimit позволяет отслеживать частоту запросов индивидуально для каждого уникального адреса отправителя, предотвращая исчерпание общего лимита одним злоумышленником.

Второй уровень защиты предполагает внесение изменений в параметры функционирования сетевого стека через конфигурационный файл /etc/sysctl.conf [4]. Перечень оптимизируемых системных переменных представлен в табл 2.

Таблица 2. Рекомендуемые значения параметров sysctl для повышения устойчивости

Системный параметр ядра	**Рекомендуемое значение**	**Ожидаемый эффект от изменения параметра**
net.ipv4.icmp_ratelimit	2000	Увеличение паузы между отправками сообщений об ошибках
net.ipv4.icmp_msgs_per_sec	100	Снижение общего объема генерируемого диагностического трафика
net.ipv4.icmp_msgs_bu	10	Уменьшение размера пикового

rst		всплеска ответов ICMP
net.ipv4.conf.all.rp_filter	1	Активация строгой фильтрации обратного пути для отсечения спуфинга
net.ipv4.conf.default.rp_filter	1	Наследование строгой фильтрации для новых сетевых интерфейсов
net.core.rmem_max	16777216	Расширение лимита буфера для защиты от переполнения
net.core.rmem_default	1048576	Увеличение стандартного размера буфера для сглаживания всплесков

Источник: анализ автора

Включение rp_filter (режим 1) обеспечивает строгую фильтрацию обратного пути, отсекая пакеты с подменными IP-адресами. Увеличение параметров rmem_max и rmem_default расширяет буферы приема, предотвращая переполнение при кратковременных всплесках трафика [5].

Третий, наиболее эффективный уровень защиты базируется на использовании технологии eBPF и расширяемого интерфейса экспресс-передачи данных XDP. Программа фильтрации, загруженная непосредственно в контекст сетевого драйвера, способна анализировать входящие заголовки и принимать решение об уничтожении мусорных UDP-пакетов до того, как ядро выделит для них память и

создаст ресурсоемкие структуры sk_buff. Экспериментальные данные показывают, что внедрение фильтров XDP позволяет успешно нейтрализовать более девяноста семи процентов атакующего трафика при минимальной нагрузке на центральный процессор, сохраняя полную доступность сервисов.

Заключение

Исследование показало, что стандартная конфигурация Astra Linux уязвима к UDP-flood: отсутствие настроек межсетевого экрана и буферизации приводит к отказу в обслуживании уже при интенсивности атаки от 100 Мбит/с из-за перегрузки ksoftirqd. Комплекс предложенных мер, ограничение частоты запросов, оптимизация параметров sysctl и внедрение фильтрации на базе eBPF XDP позволяет существенно снизить нагрузку на процессор. Реализация данных рекомендаций обеспечивает устойчивость системы к волюметрическим атакам и гарантирует стабильную работу Astra Linux в агрессивной сетевой среде.

Источники

1. **Бирих Э.В., Сахаров Д.В., Травкина Е.А.** Влияние применения файервола nftables на производительность сетевых взаимодействий в виртуализированной среде // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024). — СПб., 2025. — С. 305–309.
2. **Уваров А.В., Сахаров Д.В., Ушаков И.А.** Сравнительный анализ методов машинного обучения для обнаружения аномалий сетевого трафика // Технологии информационного общества: Сборник трудов XIX Международной отраслевой научно-технической конференции. — М., 2025. — С. 157–160.
3. **Сахаров Д.В., Бирих Э.В., Гаврилов П.Р.** Методика комплексной оценки

уровня зрелости системы информационной безопасности организации // Информационная безопасность регионов России (ИБРР-2025). — СПб., 2025. — С. 496–498.

4. **Красов А.В., Сахаров Д.В., Тасюк А.А.** Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. — 2020. — Т. 12, № 1. — С. 70–76.
5. **Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А.** Масштабируемое honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. — 2019. — Т. 5, № 3. — С. 86–97.