УДК 004.75.05

А. Ю. БЕЛОБОРОДОВ, А. В. ГОРБЕНКО, О. М. ТАРАСЮК, С. А. ШЕРЕМЕТ

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ СЕРВЕРНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Статья посвящена проблемам информационной безопасности современных компьютерных систем, которые обусловлены наличием уязвимостей в операционных системах. В качестве источника данных об уязвимостях используется агрегированная база данных, полученная в результате объединения информации из общедоступных баз данных уязвимостей: CVE и NVD. Собранные таким образом данные позволяют исследовать стадии жизненного цикла уязвимостей и проанализировать статистические данные об обнаружении и устранении уязвимостей в исследуемых операционных системах. В качестве основных направлений исследования уязвимости операционных систем в статье выделены следующие: количественная оценка обнаруженных и исправленных уязвимостей, оценка времени, которое затрачивается на устранение уязвимостей, исследование критичности уязвимостей, а также выявление общих уязвимостей в различных операционных системах.

Ключевые слова: *информационная безопасность, уязвимости операционных систем, базы данных уязвимостей, период риска, жизненный цикл уязвимости, статистика обнаружения и исправления*

Введение

На сегодняшний день вопросы обеспечения информационной безопасности являются одними из наиболее острых как для разработчиков, так и для пользователей разнообразных информационно-коммуникационных систем и услуг.

Недавним показательным примером, подчеркивающим исключительную важность данной проблемы как для систем коммерческого, так и критического использования, является хакерская атака на информационную систему пресвитерианского медицинского центра в Голливуде (Лос-Анджелес, США) [1]. В результате этой атаки была остановлена работа информационной системы госпиталя, заблокирован доступ к электронным историям болезней пациентов и результатам анализов. В больнице был введён режим чрезвычайного положения, некоторые пациенты были перевезены в другие госпитали. Ситуация была нормализована лишь через неделю, после того, как злоумышленникам был выплачен выкуп, размер которого по разным источникам варьируется от десятков тысяч долларов до нескольких миллионов.

Одной из основных причин успешных хакерских атак, информационных вторжений и вирусных эпидемия является наличие уязвимостей в программном обеспечении (ПО) информационных систем, компьютеров и коммуникационного оборудования, смартфонов и других интеллектуальных устройств. Термин «уязвимость» определён в ряде нормативных документов (ISO 27005, IETF RFC 2828) и используется рядом профильных организаций, например, NIST, ENISA, The Open Group и др. для обозначения недостатка в системе, используя который злоумышленник, может намеренно нарушить её работоспособность, целостность или конфиденциальность информации.

Уязвимость программного обеспечения является, прежде всего, результатом ошибок программирования и недостатков, допущенных при проектировании системы. Так, например, в течение первых двух с половиной месяцев 2016 года [2] компанией Microsoft было выпущено 175 обновлений, среди которых 87 – это обновления безопасности, устраняющие обнаруженные уязвимости (т.н. Security Updates), а 88 – функциональные обновления (Updates, Non-Security). Также примечательно, что для своей новейшей операционной системы Windows 10 компанией Microsoft выпущено уже более 50 обновлений безопасности [3].

Уязвимости обнаруживаются как в прикладном программном обеспечении, так и в системных модулях, а также операционных системах. В качестве примера можно упомянуть уязвимость, которая проявлялась операционных системах семейства Windows при обработке шрифтов OpenType [4]. Эксплуатация данной уязвимости позволила бы злоумышленнику запустить любое программное обеспечение на удалённом сервере. Другим примером является уязвимость, обнаруженная в криптографической библиотеке OpenSSL [5], эксплуатация которой поз-

воляла расшифровывать трафик, передаваемый по протоколу HTTPS между клиентом и сервером. Данной уязвимости в основном были подвержены операционные системы семейства Lunix.

Наиболее критическими для информационной безопасности компьютерных систем являются уязвимости операционных систем, которые компрометируют все прикладные сервисы, а также создают возможность для несанкционированного доступа к данным всех прикладных программ, хранящихся на уязвимом компьютере.

В связи с этим целью статьи является исследование уязвимости наиболее распространенных серверных операционных систем (см. табл. 1), сравнение статистики и закономерностей обнаружения и устранения уязвимостей и анализ их критичности. В статье представлены результаты исследования уязвимостей, которые были получены на основе агрегации статистических данных из двух баз данных уязвимостей – CVE и NVD [9]. Обе базы данных при описании уязвимостей используют единую систему CVE-идентификаторов.

Таблица 1

Исследуемые операционные системы

Операционная система	Дата выпуска	Версия ядра
Ubuntu Server 12.04	26.04.2012	3.2.0
Red Hat Enterprise Linux 6	10.11.2010	2.6.32
Novel Linux Enterprise Server 11 SP2	27.02.2012	3.0.13
Microsoft Windows Server 2012 R2	18.10.2012	-
Apple MacOS Server 10.8	25.06.2012	-
Oracle Sun Solaris 11	09.11.2011	-

В отличие от работ [6, 13, 14] в статье исследуется динамика изменения уязвимости конкретных программных продуктов – серверных операционных систем, а также усилия вендоров по исправлению уязвимостей. В то же время, подобные результаты, опубликованные в [7, 8] устарели и требуют существенного обновления и дополнения.

1. Жизненный цикл уязвимостей

Жизненный цикл (ЖЦ) уязвимостей наиболее детально обсуждался в работах [13–16]. Его формальное описание представлено в [13]. Как правило, все исследователи выделяют 5 базовых событий:

1) внесение уязвимости (creation);

2) обнаружение уязвимости, как правило, злоумышленниками или же экспертами по безопасности (discovery);

3) публичное раскрытие (disclosure);

4) выпуск «заплатки», т.е. исправления к программному продукту, устраняющему уязвимость (patch available);

5) устранение уязвимости в результате установки «заплатки» пользователем уязвимого ПО (patch installed).

Кроме того, между событиями 1) и 5) выделяют событие, связанное с появлением эксплойта или вредоносного ПО (вируса), автоматизирующего процесс эксплуатации уязвимости или же делающего его полностью автоматическим.

Время от момента обнаружения до момента устранения уязвимости определяют как период риска. Величина риска определяется индивидуально для конкретной компьютерной системы. В то же время одна из составляющих риска – вероятность успешной атаки на уязвимость существенно увеличивается с появлением эксплойта или же другого вредоносного ПО, эксплуатирующего данную уязвимость. Таким образом, величина риска со временем возрастает до момента выпуска «заплатки», как это показано в [14]. На величину риска также влияет наличие дополнительных средств защиты (антивирусное ПО, системы обнаружения атак, межсетевые экраны и т.п.). Кроме того, дискуссионным остается вопрос, каким образов на величину риска влияет публичное раскрытие уязвимости, т.е. публикация в открытом доступе, например, в базе данных CVE. С одной стороны злоумышленники могут воспользоваться полученной информацией для атаки на компьютерные системы, а также использовать её для разработки эксплойтов. С другой стороны пользователи, предупрежденные о наличии уязвимости, могут предпринять дополнительные меры по снижению риска информационного вторжения, а разработчики получают дополнительную информацию и стимул для скорейшего выпуска обновления.

В статье нами используется понятие «период риска», которому в [13] соответствует термин «post-disclosure risk» или «gray risk» в [16]. Этому термину соответствует временной интервал между моментом публичного раскрытия уязвимости и выпуском исправления, устраняющего эту уязвимость.

Временем публичного раскрытия уязвимости нами рассматривается дата публикации информации об уязвимости в базе данных CVE, когда каждой уязвимости присваивается уникальный CVE-идентификатор. При анализе баз данных уязвимостей CVE и NVD нами была обнаружена закономерность, что в подавляющем большинстве случаев информация об уязвимости появляется в базе данных NVD лишь после официального выпуска вендором бюллетеня безопасности, подтверждающего наличие данной уязвимости. В свою очередь выпуск бюллетеня безопасности сопровождается выпуском соответствующего обновления, устраняющего уязвимость. Таким образом, дата публикации информации об уязвимости в базе данных NVD может рассматриваться в качестве даты выпуска «заплат-

ки», а период между датой публикации информации об уязвимости в базе данных CVE и датой внесения этой информации в базу NVD – периодом риска.

2. Исследование уязвимости серверных операционных систем

В данной статье представлены результаты исследования уязвимостей по четырем направлениям:

1) количественная оценка обнаруженных и исправленных уязвимостей по каждой из операционных систем, а также сравнение динамики их обнаружения и исправления;

2) оценка величины периода риска в среднем по каждой операционной системе, а также дисперсии этой величины;

3) количественная оценка и сравнение количества уязвимостей, обнаруженных в каждой операционной системе с учетом степени их критичности;

4) выявление групповых уязвимостей, обнаруженных в нескольких ОС одновременно.

2.1. Статистика обнаружения и исправления уязвимостей

Анализ уязвимости исследуемых операционных систем был выполнен за период, начиная с 1 января 2012 года по 31 декабря 2016 года.

В таблице 3 представлены статистические данные о количестве обнаруженных и исправленных уязвимостей, информация о которых была внесена в базы CVE и NVD в течение указанного периода. Количество уязвимостей, которые были обнаружены, но не исправлены в операционных системах до 1 января 2012 года, указано в табл. 2 в строке «Начальные». В дальнейшем в статье используются следующие краткие псевдонимы исследуемых операционных систем: Ubuntu (Ubuntu Server 12.04), RedHat (Red Hat Enterprise Linux 6), Novel (Novel Linux Enterprise Server 11 SP2), Windows (Microsoft Windows Server 2012 R2), MacOS (Apple Macintosh Server 10.8), Solaris (Oracle Sun Solaris 11).

Операционные системы Red Hat Enterprise Linux 6 и Oracle Sun Solaris 11 были выпущены до рассматриваемого периода (см. табл. 2).

Релиз операционных систем Ubuntu Server 12.04, Novel Linux Enterprise server 11 SP2, Microsoft Windows Server 2012 R2 и Apple Macintosh Server 10.8 пришёлся на начало 2012 года. Примечательно, что к этому времени в предыдущих версиях этих операционных систем уже были выявлены уязвимости, которые впоследствии обнаружились и в новых версиях. Для ОС Ubuntu, таких уязвимостей было 25, для Windows – 5, для Novel – 30 и для Solaris – 9. Кроме того, в таблице 2 представлен средний уровень критичности выявленных уязвимостей (Кср.), а также среднее количество дней риска (КДРср.).

Таблица 2

Статистика уязвимости операционных систем

	Уязвимости	Ubuntu	Windows	RedHat	Novel	MacOS	Solaris
Начальные		14	0	45	26	0	9
2012	обнаружено	58	10	27	31	2	47
	исправлено	28	5	37	35	2	47
	Кср.	5.11	8.31	4.87	5.16	3.20	4.37
	КДРср.	146	132	262	112	94	89
2013	обнаружено	183	59	63	121	59	30
	исправлено	190	51	83	124	58	31
	Кср.	5.01	7.08	5.05	4.96	4.93	4.73
	КДРср.	111	130	122	101	110	75
2014	обнаружено	126	64	26	90	40	32
	исправлено	152	38	33	103	40	26
	Кср.	5.37	7.25	6.14	5.27	7.85	5.03
	КДРср.	55	91	88	51	89	75
2015	обнаружено	141	136	26	32	13	36
	исправлено	147	156	34	37	14	34
	Кср.	6.18	7.17	5.63	6.09	8.52	4.44
	КДРср.	57	101	67	71	47	92
ВСЕГО	обнаружено	522	269	187	300	114	154
	исправлено	517	250	187	299	114	138
	Кср.	5.42	7.45	5.42	5.37	6.13	4.64
	КДРср.	92	113	135	84	85	83

За исследуемых период наибольшее количество уязвимостей (522) было обнаружено в операционной системе Ubuntu Server 12.04, наименьшее (114) – в Apple Macintosh Server 10.8. Операционные системы Novel Linux Enterprise server 11 SP2 и Windows Server 2012 R2 занимают среднюю позицию.

Динамика обнаружения уязвимостей в различных операционных системах представлена на рис. 1. Для каждой из обнаруженных уязвимостей была зафиксирована дата выпуска «заплатки».

На основании данных о датах обнаружения и устранения обнаруженных уязвимостей, можно построить график «активных» уязвимостей. Этот график (рис. 2) отображает по дням количество уязвимостей, о наличии которых в каждой из операционных систем было известно, однако они не могли быть устранены, поскольку вендором ещё не была выпущена соответствующая «заплатка». Поскольку частота обнаружения новых уязвимостей значительно превышает время выпуска исправлений, которое в среднем для исследуемых операционных систем составляет 99 дней (см. табл. 2), одновременно в системе может присутствовать несколько десятков активных уязвимостей, которые предоставляют злоумышленникам благоприятную возможность для успешной атаки.

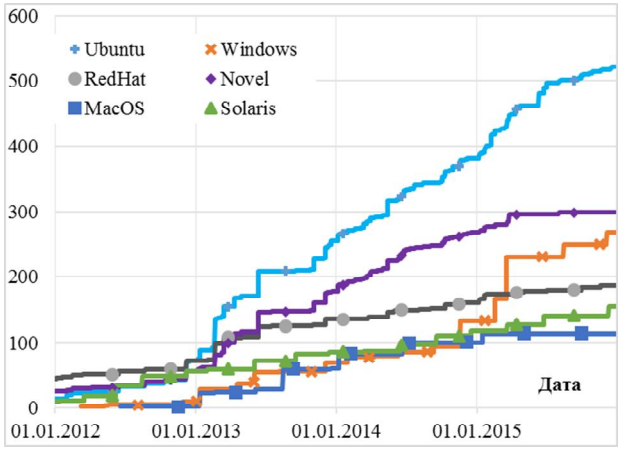

Рис. 1. Динамика обнаружения уязвимостей

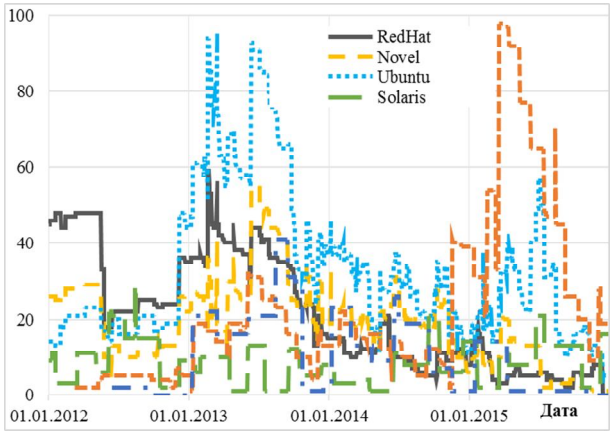

Рис. 2. Динамика изменения количества «активных» уязвимостей

Графики на рис. 2 показывают, что во время эксплуатации операционных систем практически отсутствуют периоды времени, когда в системе устранены все известные уязвимости. В течение четырех лет эксплуатации для ОС RedHat таких дней было 11, для MacOS – 159. Все остальные ОС не имели периодов времени без уязвимостей.

Очевидно, что политика профилактического прекращения эксплуатации уязвимой операционной системы до момента выпуска вендором соответствующей «заплатки» является нереалистичной из-за того, что готовность такой системы фактически оказывается равной нулю.

Таким образом, пользователи операционных систем должны принимать осознанный риск эксплуатации операционных систем, каждая из которых является потенциально уязвимой практически в любой момент времени. Сказанное является справедливым и для других видов системного и прикладного программного обеспечения.

В связи с этим особую важность в вопросах обеспечения информационной безопасности приобретает комплексное использование методов и средств антивирусной защиты, обнаружения информационных вторжений и грамотного администрирования для уменьшения вероятности успешной атаки на систему через имеющиеся в ней активные уязвимости.

2.2. Исследование периода риска

Период риска или количество дней риска (КДР) определяет количество дней, прошедших с момента обнаружения и/или публичного раскрытия уязвимости до момента выпуска вендором патча безопасности, устраняющего эту. Этот параметр является важнейшей характеристикой не только для пользователей уязвимой компьютерной системы, но и характеризует усилия, которые компания-разработчик тратит на исправление уязвимостей.

В [18] были приведены оценки, согласно которым в 1999 году период риска для продуктов компании Microsoft составлял 16 дней, RedHat – 11 дней и Sun – 90 дней. В 2006 году, согласно [19], количество дней риска для семейства операционных систем Windows (Windows 2000 (Professional and Server), and Windows XP, Windows Server 2003) возросло до 30 дней, для ОС Red Hat Enterprise Linux 2.1, 3, 4 – до 107 дней. Дополнительные приведенные оценки периода риска для Novel Linux Enterprise Server 8-10, Sun Solaris и Apple Mac OS X составили 74, 168 и 46 дней соответственно.

В 2010 году по нашим оценкам, представленным на конференции SERENE'2011, количество дней риска для ОС Windows Server 2008 возросло до 82, а для Apple MacOS Server v.10.5.8 – до 105 дней. В то же время для Oracle Solaris v.10 и RedHat Linux v.5 этот период сократился до 37 и 73 дней.

Результаты изменения среднего количества дней риска для исследуемых операционных систем в течение 2012-2016 года представлены в таблице 3.

В среднем для всех операционных систем период риска составляет 99 дней. Это означает, что после публичного раскрытия уязвимости пользователь уязвимой операционной системы ещё в течение трех месяцев остаётся фактически беззащитным перед целенаправленными хакерскими атаками.

Как следует из таблицы 2, начиная с 2012 года наблюдается тенденция к снижению периода риска практически для всех ОС, что свидетельствует о понимании компаниями разработчиками важности оперативного устранения уязвимостей. В то же время количество дней риска для современных операционных систем значительно превышает цифры 1999 [18] и 2006 [19] годов, а наихудшие показатели среди исследуемых ОС демонстрируют RedHat Enterprise Linux 6 (135) и Windows Server 2012 (113).

График функций плотности распределения вероятности количества дней риска (рис. 3), построенный по результатам статистической обработки информации из баз данных CVE и NVD позволяет оценить не только среднее значение периода риска, но и оценить вероятность исправления уязвимости в конкретный момент времени после её обнаружения.

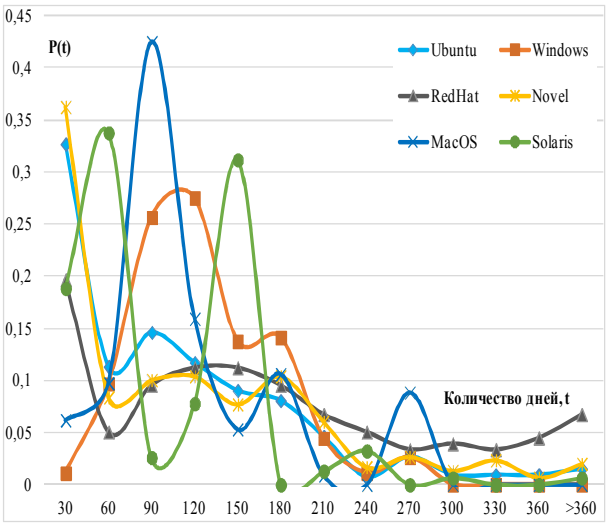

Рис. 3. Вероятность устранения уязвимости в течение периода риска

2.3. Критичность уязвимостей

Наряду со средним числом дней, затрачиваемых на устранение уязвимости, при оценке безопасности компьютерных систем необходимо учитывать критичность обнаруживаемых уязвимостей. Данный показатель, согласно системе оценивания критичности CVSS [20], варьируется в интервале от 0 до 10, где значение 10 соответствует самым опасным уязвимостям. Динамика изменения данного показателя для различных ОС в течение 2012-2015 гг. представлена в табл. 3, а общее распределение количества уязвимостей по уровням критичности представлено на рис. 4. В среднем, наименее критическими являются уязвимости операционной системы Oracle Solaris (4,13). Наибольший уровень критичности имеют уязвимости в ОС Microsoft Windows (6,46) и Apple MacOS (5,27). Кроме того, количество уязвимостей с повышенным уровнем критичности (8–10) для ОС Windows составляет почти 30%, для Solaris – 15 процентов. Для других операционных систем количество таких уязвимостей не превышает 10%. В процессе исследований нами была проверена гипотеза о том, что компании-разработчики уделяют большее внимание устранению наиболее критических уязвимостей. Однако диаграммы, представленные на рис. 5, показывают, что количество дней риска фактически не зависит от степени критичности уязвимости. Более того, время выпуска исправлений для наиболее критических уязвимостей в ОС Oracle Solaris занимает, в среднем, в три раза больше, чем время исправления всех других уязвимостей. Также видно, что время устранения уязвимостей, кроме наиболее критических, в ОС RedHat в среднем в 1,5-2 раза превышает время устранения уязвимостей других операционных систем.

Таблица 3

Критичность уязвимостей операционных систем

	Критичность	1	2	3	4	5	6	7	8	9	10
2012	Ubuntu	3	4	1	20	11	11	6		1	1
	Windows					2		2		5	1
	RedHat	3	3	2	7	4	4	2		1	1
	Novel	2	3	1	11	2	8	2		1	1
	MacOS		1		1						
	Solaris	2	6	12	13	7	2	4	1		
	Всего:	**10**	**17**	**16**	**52**	**26**	**25**	**16**	**1**	**8**	**4**
2013	Ubuntu	18	13	6	65	23	29	23	1	2	3
	Windows			1	6	7	5	29		9	2
	RedHat	10	3	1	18	7	15	7			2
	Novel	14	11	5	40	11	19	17		1	3
	MacOS	3	9	3	18	7	16	3			
	Solaris	3	3		17	1	2	3			1
	Всего:	**48**	**39**	**16**	**164**	**56**	**86**	**82**	**1**	**12**	**11**
2014	Ubuntu	4	9	1	54	15	16	23			4
	Windows	3	3	1	9	6	6	16	1	17	2
	RedHat	1	1	1	5	4	4	6		1	3
	Novel	1	9	2	44	8	10	12			4
	MacOS		1	1	3	2	21	3		1	8
	Solaris	1	3	1	13	5	3	6			
	Всего:	**10**	**26**	**7**	**128**	**40**	**60**	**66**	**1**	**19**	**21**
2015	Ubuntu	1	6	8	22	29	18	37	1	8	11
	Windows	3	19	2	8	8	11	48		35	2
	RedHat		4		2	7	6	7			
	Novel		6	1	7	2	2	6		2	6
	MacOS	2					4	6			1
	Solaris	5	3	5	13	1	4	5			
	Всего:	**11**	**38**	**16**	**52**	**47**	**45**	**109**	**1**	**45**	**20**
Итого	Ubuntu	26	32	16	161	78	74	89	2	11	19
	Windows	6	22	4	23	23	22	95	1	66	7
	RedHat	14	11	4	32	22	29	22	0	2	6
	Novel	17	29	9	102	23	39	37	0	4	14
	MacOS	5	11	4	22	9	41	12	0	1	9
	Solaris	11	15	18	56	14	11	18	1	0	1
	Всего:	**79**	**120**	**55**	**396**	**169**	**216**	**273**	**4**	**84**	**56**

2.4. Исследование общих уязвимостей

Наибольшую опасность среди уязвимостей представляют такие, которые присутствуют одновременно в нескольких операционных системах.

Причиной появления групповых уязвимостей является использование различными ОС одних и тех же уязвимых программных компонентов (например, системных библиотек или модулей ядра операционной системы).

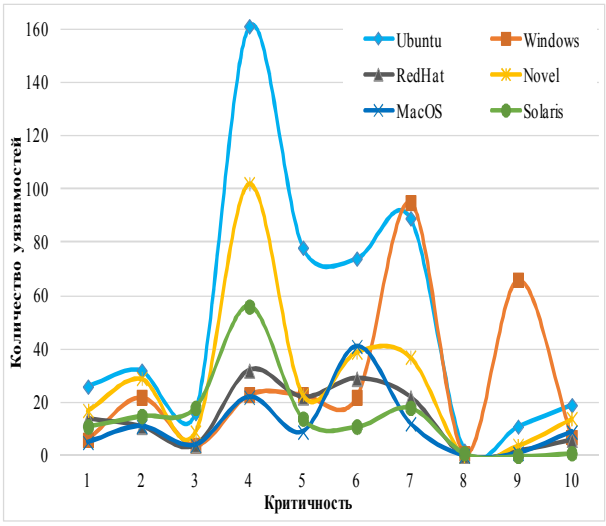

Рис. 4. Количественное распределение уязвимостей по уровням критичности

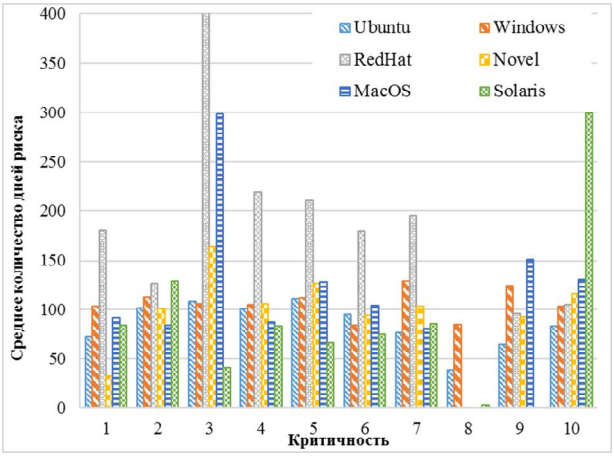

Рис. 5. Количество дней риска уязвимостей разного уровня критичности

Чаще всего общие уязвимости обнаруживаются в «родственных» операционных системах, например, различных версиях ОС Windows, разных ОС семейства Linux (RedHat, Novel, Ubuntu) или же Unix (OpenBSD, FreeBSD, NetBSD).

Тем не менее, периодически обнаруживаются уязвимости, общие для различных семейств операционных систем. Например, уязвимость CVE-2008-4609, позволявшая удаленному злоумышленнику успешно выполнить атаку типа «отказ в обслуживании», была обнаружена одновременно в ОС Linux, BSD Unix, Microsoft Windows, Cisco IOS и, возможно, некоторых других. Уязвимость заключалась в наличии алгоритмической ошибки в реализации протокола TCP, которая позволяла добиться переполнения очереди TCP-соединений на основе манипуляции значением флагов в заголовке TCP-сегмента. В результате проведенного анализа нами были обнаружены многочисленные общие уязвимости для трех ОС семейства Linux (см. рис. 6)

В период с 2012 по 2015 гг. нами было выявлено 47 абсолютных общих уязвимостей, которые были обнаружены во всех трех операционных системах: Ubuntu, Novel и RedHat. Наибольшую степень диверсности с точки зрения наличия групповых уязвимостей демонстрируют Novel и RedHat, в то время как Ubuntu и Novel имеют более 200 совместных уязвимостей. Подавляющее большинство общих уязвимостей относятся к уязвимостям ядра Linux указанных операционных систем.

Кроме того была выявлена одна уязвимость в SOAP-парсере модуля PHP (CVE-2013-1848), общая для RedHat и MacOS, которая позволяла получить неавторизованный доступ к произвольным файлам компьютерной системы.

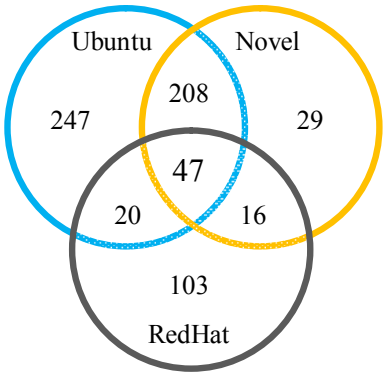

Рис. 6. Количество индивидуальных, общих абсолютных и групповых уязвимостей в ОС семейства Linux

Выводы

В статье представлены результаты ретроспективного анализа уязвимости наиболее распространенных серверных операционных систем: Ubuntu Server 12.04, Red Hat Enterprise Linux 6, Novel Linux Enterprise Server 11 SP2, Microsoft Windows Server 2012 R2, Apple MacOS Server 10.8 и Oracle Sun Solaris 11. Для проведения такого анализа использовалась статистическая информация из баз данных уязвимостей CVE и NVD.

Одними из основных показателей, влияющих на безопасность компьютерных систем, является не только количество обнаруженных уязвимостей и их критичность, но и время (т.н. период риска), которое требуется компании-разработчику для выпуска «заплатки», устраняющей уязвимость.

Как показал проведенный анализ, среднее значение периода риска для исследуемых ОС варьируется от 83 (Oracle Solaris) до 135 (Red Hat) дней, что предоставляет серьёзную угрозу информационной безопасности и обуславливает необходимость комплексного эшелонированного применения различ-

ных методов и средств защиты (антивирусов, межсетевых экранов, систем обнаружения атак и т.п.).

Кроме того, нами был установлен тот факт, что интенсивность разработки вендорами патчей безопасности фактически не зависит от уровня критичности уязвимостей, что указывает на несовершенство организации процесса их устранения компаниями-разработчиками. Также, беспокойство вызывает факт увеличения количества уязвимостей с высоким уровнем критичности для всех операционных систем.

В заключении статьи были исследованы групповые уязвимостей, проявляющиеся более чем в одной операционной системе. Наличие таких уязвимостей может приводить к масштабным атакам и вирусным эпидемиям, а также усложняет построение отказоустойчивых информационных систем, реализующих принцип диверсности программного обеспечения.

Результаты, представленные в работе, позволяют оценить уровень современных информационных угроз, обусловленных наличием уязвимостей в программном обеспечении компьютерных систем и оценить безопасность использования различных операционных систем.

Литература

1. В США хакеры вывели больницу из строя и требуют выкуп [Электронный ресурс]. – Режим доступа: http://lenta.ru/news/2016/02/16/hospitaloffline/. – 20.03.2016.

2. Description of Software Update Services and Windows Server Update Services changes in content for 2016 [Электронный ресурс]. – Режим доступа: https://support.microsoft.com/en-us/kb/894199. – 20.03.2016

3. Vulnerability Summary for CVE-2013-1291 [Электронный ресурс]. – Режим доступа: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1291 – 20.03.2016.

4. Бюллетень по безопасности Microsoft [Электронный ресурс]. – Режим доступа: https://technet.microsoft.com/ru-ru/security/bulletin/dn602597.aspx. – 20.03.2016

5. Vulnerability Summary for CVE-2014-0160 [Электронный ресурс]. – Режим доступа: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160 – 20.03.2016.

6. OS Diversity for Intrusion Tolerance: Myth or Reality? [Текст] / M. Garcia, A. Bessani, I. Gashi, etc. // Proc. 2011 IEEE/IFIP 41st Int. Conf. on Dependable Systems & Networks (DSN'2011), 2011. – P. 383–394.

7. Jones, J. Days-of-risk in 2006: Linux, Mac OS X, Solaris and Windows [Электронный ресурс]. – Режим доступа: http://blogs.csoonline.com/days_of_risk_in_2006 – 20.03.2016

8. Using Diversity in Cloud-Based Deployment Environment to Avoid Intrusions [Текст] / A. Gorbenko, O. Tarasyuk, V. Kharchenko, A. Romanovsky // Software Engineering for Resilient Systems, LNCS 6968 / E. Troubitsyna. – Berlin, Heidelberg (Germany): Springer-Verlag, 2011. – P. 145–155.

9. Белобородов, А. Ю. Применение баз данных уязвимостей в задачах исследования безопасности программных средств [Текст] / А. Ю. Белобородов, А. В. Горбенко // Вісник Харківського національного університету сільського господарства ім. Петра Василенка. – 2015. – № 165. – С. 83-85.

10. Modelling the Security Ecosystem - The Dynamics of (In)Security [Text] / S. Frei, D. Schatzmann, B. Plattner, B. Trammell // In: Economics of Information Security and Privacy / T. Moore, D. Pym, C. Ioannidis (Eds.). – Springer, 2010. – P. 79–106.

11. Basic Guide to Days of Risk [Электронный ресурс]. – Режим доступа: http://www.csoonline.com/article/2136934/data-protection/basic-guide-to-days-of-risk.html. – 20.03.2016.

12. Jones, J. R. Putting Days-of-Risk to Practical Use [Электронный ресурс] / J. R Jones. – Режим доступа: https://technet.microsoft.com/en-us/library/dd277347.aspx. – 20.03.2016.

13. Large-scale vulnerability analysis [Text] / S. Frei, M. May, U. Fiedler et al // Proc. SIGCOMM Workshop on Large-Scale Attack Defense. – 2006. – P. 131–138.

14. Shahzad, M. A large scale exploratory analysis of software vulnerability life cycles [Текст] / M. Shahzad, M. Zubair Shafiq, A. X. Liu // Proc. 34th Int. Conf. on Software Engineering (ICSE '12). – 2012. – P. 771–781.

15. Reavis, J. Linux vs. Microsoft: Who Solves Security Problems Faster? [Электронный ресурс] / J. Reavis. – 2010. – Режим доступа: http://www.reavis.org/research/solve.shtml. – 20.03.2016.

16. Jones, J. Days-of-risk in 2006 : Linux, Mac OS X, Solaris and Windows [Электронный ресурс] / J. Jones. – 2007. – Режим доступа: http://www.csoonline.com/article/2136935/data-protection/days-of-risk-in-2006---linux--mac-os-x--solaris-and-windows.html. – 20.03.2016.

17. A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0 [Электронный ресурс]. – Режим доступа: http://www.first.org/cvss/cvss-guide.html. – 20.03.2016.

18. Reavis, J. Linux vs. Microsoft: Who Solves Security Problems Faster? [Электронный ресурс] / J. Reavis. – 2010. – Режим доступа: http://www.reavis.org/research/solve.shtml. – 20.03.2016.

19. Jones, J. Days-of-risk in 2006 : Linux, Mac OS X, Solaris and Windows [Электронный ресурс] / J. Jones. – 2007. – Режим доступа: http://www.csoonline.com/article/2136935/data-protection/days-of-risk-in-2006---linux--mac-os-x--solaris-and-windows.html. – 20.03.2016.

20. A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0 [Электронный ресурс]. – Режим доступа: http://www.first.org/cvss/cvss-guide.html. – 20.03.2016.

References

1. *V SShA hakery vyveli bol'nicu iz stroja i trebujut vykup* [In the USA hackers have attacked a hospital and require a ransom]. Available at: http://lenta.ru/news/2016/02/16/hospitaloffline/ (accessed 20.03.2016) (In Russian)
2. *Description of Software Update Services and Windows Server Update Services changes in content for 2016.* Available at: https://support.microsoft.com/en-us/kb/894199 (accessed 20.03.2016)
3. *Vulnerability Summary for CVE-2013-1291.* Available at: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1291 (accessed 20.03.2016)
4. *Bjulleten' po bezopasnosti Microsoft* [Security Bulletin]. Available at: https://technet.microsoft.com/ru-ru/security/bulletin/dn602597.aspx (accessed 20.03.2016) (In Russian)
5. *Vulnerability Summary for CVE-2014-0160.* Available at: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160 (accessed 20.03.2016)
6. Garcia, M., Bessani, A., Gashi, I., etc. OS Diversity for Intrusion Tolerance: Myth or Reality? *Proc. 2011 IEEE/IFIP 41st Int. Conf. on Dependable Systems & Networks (DSN'2011)*, 2011, pp. 383–394.
7. Jones, J. *Days-of-risk in 2006: Linux, Mac OS X, Solaris and Windows.* Available at: http://blogs.csoonline.com/days_of_risk_in_2006 (accessed 20.03.2016)
8. Gorbenko, A., Tarasyuk, O., Kharchenko, V., Romanovsky, A. Using Diversity in Cloud-Based Deployment Environment to Avoid Intrusions. *Software Engineering for Resilient Systems, LNCS 6968 / E. Troubitsyna,* Berlin, Heidelberg (Germany), Springer-Verlag Publ., 2011, pp. 145–155.
9. Beloborodov, A. Ju., Gorbenko A. V. Primenenie baz dannyh ujazvimostej v zadachah issledovanija bezopasnosti programmnyh sredstv [The use of database vulnerability research in problems of software security]. *Visny`k Xarkivs`kogo nacional`nogo universy`tetu sil`s`kogo gospodarstva imeni Petra Vasy`lenka,* 2015. no. 165, pp. 83-85 (In Russian)
10. Frei, S., Schatzmann, D., Plattner, B., Trammell, B. Modelling the Security Ecosystem - The Dynamics of (In)Security. In: *Economics of Information Security and Privacy,* Springer Publ., 2010, pp. 79–106.
11. *Basic Guide to Days of Risk.* Available at: http://www.csoonline.com/article/2136934/data-protection/basic-guide-to-days-of-risk.html (accessed 20.03.2016)
12. Jones, J. R. Putting Days-of-Risk to Practical Use. Available at: https://technet.microsoft.com/en-us/library/dd277347.aspx (accessed 20.03.2016)
13. Frei, S., May, M., Fiedler, U. et al Large-scale vulnerability analysis. *SIGCOMM Workshop on Large-Scale Attack Defense*, 2006, pp. 131–138.
14. Shahzad, M. Zubair, Shafiq M., Liu, A. X. A large scale exploratory analysis of software vulnerability life cycles. *Proc. 34th Int. Conf. on Software Engineering (ICSE '12)*, 2012, pp. 771–781.
15. Reavis, J. *Linux vs. Microsoft: Who Solves Security Problems Faster?* Available at: http://www.reavis.org/research/solve.shtml (accessed 20.03.2016)
16. Jones, J. *Days-of-risk in 2006 Linux, Mac OS X, Solaris and Windows.* Available at: http://www.csoonline.com/article/2136935/data-protection/days-of-risk-in-2006---linux--mac-os-x--solaris-and-windows.html (accessed 20.03.2016)
17. *A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0.* Available at: http://www.first.org/cvss/cvss-guide.html (accessed 20.03.2016)
18. Reavis, J. *Linux vs. Microsoft: Who Solves Security Problems Faster?*, 2010. Available at: http://www.reavis.org/research/solve.shtml (accessed 20.03.2016)
19. Jones, J. *Days-of-risk in 2006: Linux, Mac OS X, Solaris and Windows*, 2007. Available at: http://www.csoonline.com/article/2136935/data-protection/days-of-risk-in-2006---linux--mac-os-x--solaris-and-windows.html (accessed 20.03.2016)
20. *A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0.* Available at: http://www.first.org/cvss/cvss-guide.html (accessed 20.03.2016)

Поступила в редакцию 21.03.2016, рассмотрена на редколлегии 14.04.2016

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ

О. Ю. Білобородов, А. В. Горбенко, О. М. Тарасюк, С. О. Шеремет

Стаття присвячена проблемам інформаційної безпеки сучасних комп'ютерних систем, які зумовлені наявністю вразливостей в операційних систем. В якості джерела даних про вразливості використовується агрегована база даних, яка отримана в результаті об'єднання інформації з загальнодоступних баз даних вразливостей: CVE та NVD. Зібрані таким шляхом дані дозволяють дослідити стадії життєвого циклу вразливостей та виконати аналіз статистичних даних щодо виявлення та усунення вразливостей в різних операційних системах. В якості основних напрямків дослідження вразливості операційних систем в статті виділено наступні: кількісна оцінка виявлених та виправлених вразливостей, оцінка часу, який витрачається на виправлення вразливостей, дослідження критичності вразливостей, а також виявлення загальних вразливостей в різних операційних системах.

Ключові слова: інформаційна безпека, вразливості операційних систем, бази даних вразливостей, період ризику, життєвий цикл вразливостей, статистика виявлення та виправлення

SERVER OPERATING SYSTEM VULNERABILITIES INVESTIGATION

O. Y. Biloborodov, A. V. Gorbenko, O. M. Tarasyuk, S. A. Sheremet

In the paper we analyse security problems of modern computer systems caused by vulnerabilities in their operating systems. An aggregated vulnerability database has been developed by joining vulnerability records from different publicly available vulnerability databases: CVE and NVD. Aggregated data allow us to investigate vulnerability life cycle stages and to analyze vulnerability disclosure and elimination statistics for different operating systems. Main operating systems security issues considered in the paper are: quantitative assessment of discovered and fixed vulnerabilities, estimation of a time that each vendor spends on patch issuing, analysis of vulnerabilities criticality and discovery of common vulnerabilities in different operating systems.

Keywords: security, operating system vulnerabilities, vulnerability databases, days of risk, vulnerability life cycle, disclosure and elimination statistics

Белобородов Александр Юрьевич – аспирант кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: A.Beloborodov@csn.khai.edu.

Горбенко Анатолий Викторович – д-р техн. наук, профессор, декан факультета радиотехнических систем летательных аппаратов Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: A.Gorbenko@csn.khai.edu.

Тарасюк Ольга Михайловна – канд. техн. наук, доцент, доцент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: O.Tarasyuk@csn.khai.edu.

Шеремет Сергей Александрович – аспирант кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: S.Sheremet@csn.khai.edu.

Beloborodov Alexander – PhD Student at Department of Computer Systems and Networks, National Aerospace University named after N. Ye. Zhukovsky "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: A.Beloborodov@csn.khai.edu.

Gorbenko Anatoliy – Dr.Sc., Professor, Dean of the Aircraft Radio-Technical Faculty, National Aerospace University named after N. Ye. Zhukovsky "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: A.Gorbenko@csn.khai.edu.

Tarasyuk Olga – PhD, Docent, Associate Professor with the Department of Computer Systems and Networks, National Aerospace University named after N. Ye. Zhukovsky "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: O.Tarasyuk@csn.khai.edu.

Sheremet Sergey – PhD Student with the Department of Computer Systems and Networks, National Aerospace University named after N. Ye. Zhukovsky "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: S.Sheremet@csn.khai.edu.