Всего строк — 290, показаны 20 строк

/.svn/
/.svn/text-base/
/ban/
/bitrix/cache/
/bitrix/cache/css/
/bitrix/cache/css/s1/
/bitrix/cache /css/s1/boguchar_new/
/bitrix/cache/css/s1/boguchar_new/page_80f98023e41dadd741c628b70c6ce315/
/bitrix/cache/css/s1/boguchar_new/template_ 799621fa1088210b7c1524a995f66a57/
/bitrix/cache /css/s1/sitea_contrast/
/bitrix/cache /css/s1/sitea_contrast/kernel_main/
/bitrix/cache/css/s1/sitea_contrast/page_5d340d32c5742a37bf0533c1adcfa628/
/bitrix/cache/css/s1/sitea_contrast/page_80f98023e41dadd741c628b70c6ce315/
/bitrix/cache/css/s1/sitea_contrast/page_da5998554eecc2db68f602bf3d0b2cf3/
/bitrix/cache/css/s1/sitea_contrast/templat e_b8b08d60d0be00aae97882dc400393e7/
/bitrix/cache/js/
/bitrix/cache/js/s1/
/bitrix/cache /js/s1/sitea_contrast/
/bitrix/cache /js/s1/sitea_contrast/kernel_main/
/bitrix/cache/js/s1/sitea_contrast/page_1d3616f9a2f2c6548c1532cec6594c55/

Всего строк — 290, показаны 20 строк

CVSS
Базовая оценка 2.1 (AV:N/AC:H/Au:S/C:P/I:N/A:N)

Низкий уровень
Список документов
ID: 1285

Описание
Список документов, найденных на веб-сервере:

/news/documents/2017/july/PSP°%20CЃP°PN°C,%20Ps%20CЃPsPIPµC‰P°PSPëPë%2003%20PëCЂP»CЏ.doc
/news/documents/2017/july/PќPsPIPsCЃC,Pë%202%20CЃ.doc

CVSS
Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

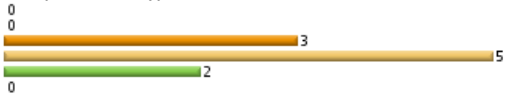
IP адрес
193.109.247.229

Имя из задачи
www.butoo.narod.ru

FQDN
dev.ucoz.net

Уязвимых служб/ПО: **2**

Распределение уровней опасности



80/TCP - HTTP

Имя сервера:	nginx/1.8.0
Состояние:	200 (OK)
Имя сервера (определено эвристикой):	Nginx HTTP Server

Информация об имени приложения подтверждена эвристическим методом

Уязвимость
Межсайтовое выполнение сценариев
ID: 1290

Описание

Уязвимость в расширении Adobe Reader для популярных браузеров позволяет злоумышленникам провести атаку "межсайтовое выполнение сценариев" на любой веб-сервер, на котором хранятся документы в формате PDF. Для успешной эксплуатации уязвимости необходимо, чтобы пользователь перешел по специально сформированной ссылке; тогда вредоносный код будет выполнен в контексте безопасности сайта, на котором расположен PDF-документ.
Пример запроса:
http://site/file.pdf#filed=javascript:alert()

Как исправить

Возможны различные варианты решения.
Файлы PDF могут быть удалены с сайта или перемещены в архивные файлы.
Ещё одним вариантом является замена заголовка Content-Type в ответе сервера или добавление заголовка Content-Disposition: attachment. В web-сервере Apache для этого можно использовать следующие строки в httpd.conf:
Header unset Content-Disposition
Header add Content-Disposition "attachment"
Клиенты должны установить Adobe Reader 8 и выше:
http://www.adobe.com/products/acrobat/readstep2.html

CVSS

Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Ссылки

http://www.securityfocus.com/bid/21858/references
http://www.kb.cert.org/vuls/id/815960
http://www.wisec.it/vulns.php?page=9
http://www.adobe.com/support/security/advisories/apsa07-01.html

---

Уязвимость
Незащищенная передача данных
ID: 1273

Описание

Обнаружены формы, которые могут передавать конфиденциальные данные на сервер в незащищенном виде. Протокол HTTP является небезопасным, так как весь трафик (включая пароли пользователей) передается между компьютерами в незашифрованном виде и может быть перехвачен путем прослушивания сети.
Список форм:

```
POST /panel/sub/ HTTP/1.1

user=&password=&dnsc=0Y61B89sJTQweW0dz^JH$5jFwQs86OBPpr8XHzTwlgoo&submlform=&a=dologin&ss=1
```

Как исправить

Используйте защищенный протокол TLS 1.1 или TLS 1.2 для передачи конфиденциальной информации на сервер.

CVSS

Базовая оценка 3.3 (AV:A/AC:L/Au:N/C:P/I:N/A:N)

Уязвимость
Список невидимых ссылок
ID: 1265

Описание

Список невидимых ссылок, обнаруженных на веб-сервере с использованием словаря:

```
<a href="http://www.butoo.narod.ru/admin/" target=_blank>/admin/</a>
<a href="http://www.butoo.narod.ru/stat/" target=_blank>/stat/</a>
```

Как исправить

Удалите ненужные файлы и каталоги.

CVSS

Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

Низкий уровень
Доступ к каталогам
ID: 1013

Описание

Были обнаружены следующие доступные каталоги:

```
<a href="http://www.butoo.narod.ru/admin/" target=_blank>/admin/</a>
<a href="http://www.butoo.narod.ru/mail/" target=_blank>/mail/</a>
<a href="http://www.butoo.narod.ru/secure/" target=_blank>/secure/</a>
```

/slab/
/stat/

CVSS
Базовая оценка 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Низкий уровень
Список документов
ID: 1285

Описание
Список документов, найденных на веб-сервере:

/dokum/Instr_po_rab_s_obr_grazhdan.doc
/dokum/goryachaya_liniya_ORVI.pdf
/dokum/mun_prog/Post_1421.doc
/dokum/mun_prog/Post_479.doc
/dokum/prik_1025.pdf
/dokum/rek_po_sokr_otchetnosti.pdf

CVSS
Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

80/TCP - nginx • Версия: 1.8.0

Подозрение на уязвимость
Использование после освобождения
ID: 185694
CVE: CVE-2016-0746
Дата публикации: 26.01.2016

Краткое описание
Уязвимость позволяет атакующему вызвать аварийное завершение рабочего процесса.

Описание
Использование после освобождения при обработке ответа CNAME позволяет злоумышленникам вызвать аварийное завершение рабочего процесса или оказать иное воздействие на систему, вызвав преобразование имен.

Как исправить
Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу:
http://nginx.org

CVSS
Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Временная оценка 3.7 (AV:N/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C)

Ссылки
http://mailman.nginx.org/pipermail/nginx-announce/2016/000169.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0746

Подозрение на уязвимость
Отказ в обслуживании
ID: 185693
CVE: CVE-2016-0742
fstec: BDU:2016-00707
Дата публикации: 26.01.2016

Краткое описание
Уязвимость позволяет атакующему вызвать аварийное завершение рабочего процесса.

Описание
Разыменование недопустимого указателя при обработке ответа DNS-сервера позволяет злоумышленникам вызвать аварийное завершение рабочего процесса, используя специально сформированные UDP-пакеты.

Как исправить
Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу:
http://nginx.org

CVSS
Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Временная оценка 3.7 (AV:N/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C)

Ссылки
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0742

http://mailman.nginx.org/pipermail/nginx-announce/2016/000169.html

---

Подозрение на уязвимость
Отказ в обслуживании
ID: 185695
CVE: CVE-2016-0747
Дата публикации: 26.01.2016

Краткое описание
Уязвимость позволяет атакующему вызвать чрезмерное потребление ресурсов.

Описание
Уязвимость, связанная с некорректными ограничениями преобразований CNAME, позволяет злоумышленникам вызвать чрезмерное потребление ресурсов в рабочих процессах, вызвав преобразование произвольного имени.

Как исправить
Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу:
http://nginx.org

CVSS
Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Временная оценка 3.7 (AV:N/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C)

Ссылки
http://mailman.nginx.org/pipermail/nginx-announce/2016/000169.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0747

Подозрение на уязвимость
Отказ в обслуживании
ID: 186285
CVE: CVE-2016-4450
Дата публикации: 07.06.2016

Краткое описание
Уязвимость позволяет злоумышленнику вызвать отказ в обслуживании (разыменование нулевого указателя и аварийное завершение рабочего процесса).

Описание
Уязвимость в os/unix/ngx_files.c в nginx позволяет злоумышленникам, действующим удаленно, вызвать отказ в обслуживании (разыменование нулевого указателя и аварийное завершение рабочего процесса), используя специально сформированный запрос и запись тела запроса клиента во временный файл.

Как исправить
Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу:
http://nginx.org/

CVSS
Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Временная оценка 3.7 (AV:N/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C)

Ссылки
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4450
http://mailman.nginx.org/pipermail/nginx-announce/2016/000179.html

---

Подозрение на уязвимость
Целочисленное переполнение
ID: 188629
CVE: CVE-2017-7529
Дата публикации: 11.07.2017

Краткое описание
Уязвимость позволяет злоумышленнику получить доступ к конфиденциальной информации.

Описание
Уязвимость в фильтре диапазонов nginx позволяет злоумышленникам вызвать целочисленное переполнение и получить доступ к конфиденциальной информации при помощи специально сформированного запроса.

Как исправить
Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу:
https://nginx.org/

CVSS
Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Временная оценка 3.7 (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:U/RL:OF/RC:C)

Ссылки
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7529
http://mailman.nginx.org/pipermail/nginx-announce/2017/000200.html

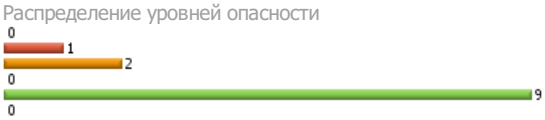
IP адрес
92.53.96.168

FQDN
vh104.timeweb.ru

Имя из задачи
www.butur-rn.ru

Уязвимых служб/ПО: **3**

Распределение уровней опасности



80/TCP - PHP ● Версия: 5.3.29

Подозрение на серьезную уязвимость
Неподдерживаемая версия
ID: 186963

Краткое описание
Данная версия продукта более не поддерживается разработчиками.

Описание
Данная версия продукта может содержать критические уязвимости, но срок ее поддержки истек и разработчики более не выпускают обновлений безопасности.

Как исправить
Рекомендуется установить последнюю версию продукта. Необходимую информацию можно получить по адресу: https://secure.php.net/

CVSS
Базовая оценка 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Ссылки
https://secure.php.net/eol.php

80/TCP - HTTP

Имя сервера:	nginx/1.14.0 - PHP/5.3.29 - Bitrix Site Manager
Состояние:	200 (OK)
Имя сервера (определено эвристикой):	Nginx HTTP Server

Информация об имени приложения подтверждена эвристическим методом

Уязвимость
Незащищенная передача данных
ID: 1273

Описание
Обнаружены формы, которые могут передавать конфиденциальные данные на сервер в незащищенном виде. Протокол HTTP является небезопасным, так как весь трафик (включая пароли пользователей) передается между компьютерами в незашифрованном виде и может быть перехвачен путем прослушивания сети.
Список форм:

```
POST /bitrix/admin/fileman_html_edit.php?path=/econom/otdel_po_mobilizacii_dokhodov/index.php&site=s1&lang=ru&filter=Y&set_filter=Y HTTP/1.1

AUTH_FORM=Y&TYPE=AUTH&USER_LOGIN=&USER_PASSWORD=&Login=&captcha_sid=&captcha_word=&USER_REMEMBER=Y&sessid=02b9a4d6be1e1c70b1e8a62d2e45f66a
```

Как исправить
Используйте защищенный протокол TLS 1.1 или TLS 1.2 для передачи конфиденциальной информации на сервер.

CVSS
Базовая оценка 3.3 (AV:A/AC:L/Au:N/C:P/I:N/A:N)

Низкий уровень
Доступ к каталогам
ID: 1013

Описание
Были обнаружены следующие доступные каталоги:

Всего строк — 264, показаны 20 строк