آزمایشگاه آپا

آگاهی‌رسانی، پشتیبانی و امداد در

حوزه امنیت سیستم‌عامل

دانشگاه صنعتی امیرکبیر

(با حمایت مرکز تحقیقات مخابرات ایران)

گروه مدیریت

فرمهای گزارش دهی و ذخیره حوادث

FC_۸۷_۰۶_۰۹

تاریخ: ۸۷/۰۶

مشخصات سند			
نام سند: فرمهای گزارش دهی و ذخیره حوادث			
کد فایل	**آخرین نسخه**	**تاریخ آخرین بازبینی**	**گروه**
FC_۸۷_۰۶_۰۹	۱،۱	۸۷/۰۸/۱۸	مدیریت

سابقه سندها			
نسخه	**تاریخ تنظیم**	**تنظیم‌کننده**	**توضیحات**
۱،۰	۸۷/۰۶/۲۷	خدیجه محمدزاده	ایجاد

چکیده

در این گزارش فرمهایی برای گزارش دهی،ذخیره سازی و گزارش نهایی پس از رفع حادثه ارائه شده است.این فرمها باید مطابق با نیازها و سرویسهای OS-CERT تغییر داده شوند.

فهرست مطالب

۱ فرم گزارش حادثه ۱

۲ فرم گزارش آسیب پذیری ۲

۳ سیستم گزارش حادثه مبتنی بر وب ۴

۴ فرم پاسخ به حادثه ۱۰

۵ فرم گزارش نهایی پس از رفع حادثه ۲۱

۶ منابع و مراجع ۲۴

۱ فرم گزارش حادثه

اطلاعات تماس

۱.نام

۲.نام سازمان

۳.نوع بخش (به عنوان مثال بانکی ، آموزشی، انرژی)

۴.آدرس پست الکترونیک

۵.شماره تلفن

۶.سایر

سیستمهای تاثیر دیده

۷.نام کامپیوتر میزبان و IP :

۸.ناحیه زمانی :

۹.هدف یا وظیفه کامپیوتر میزبان (لطفا تا حد ممکن دقیق باشد):

مبدا حمله

۱۰.نام کامپیوتر میزبان یا IP :

۱۱.ناحیه زمانی:

۱۲.درتماس بوده است؟

۱۳.تخمین هزینه پاسخگویی به حادثه (در صورت آگاهی)

۱۴.توضیح حادثه (شامل تاریخ، متدهای نفوذ، ابزارهای مورد استفاده، نسخه نرم افزار و سطح وصله، خروجی ابزار نفوذ، جزئیات آسیب پذیریهایی که مورد استفاده قرار گرفته اند، مبدا حمله و دیگر اطلاعات مربوط به حادثه)

۲ فرم گزارش آسیب پذیری

اطلاعات تماس

نام:

پست الکترونیک:

تلفن/فاکس:

سازمان و آدرس:

آیا این آسیب پذیری را به تولیدکنندگان محصول گزارش کرده اید؟ [بله/ خیر]

اگر گزارش کرده اید لطفا اطلاعات تماس کسانی که با آنها ارتباط برقرار کرده اید را ذکر کنید:

تاریخ گزارش:

نام تماس تولیدکننده:

شماره تماس تولید کننده:

پست الکترونیک تولیدکننده:

شماره ارجاع تولیدکننده:

اگر شما می خواهید که این گزارش بی نام باقی بماند در کنار عبارت زیر علامت تیک بزنید.

_ هویت مرا برای تولید کننده منتشر نسازید.

اطلاعات فنی

اگر شماره پیگیری آسیب پذیری CERT وجود دارد لطفا آن را ذکر کنید.

لطفا آسیب پذیری را توضیح دهید.

تاثیر این آسیب پذیری چیست؟ (به عنوان مثال کاربر محلی می تواند به دسترسی در سطح ریشه برسد، حمله ممانعت از سرویس و غیره)

A)تاثیر خاص جیست؟

B)آسیب پذیری چگونه در حمله مورد استفاده قرار گرفته است؟

آیا آسیب پذیری اکنون مورد بهره برداری قرار گرفته است؟

اگر کد استثمارگر دردسترس است لطفا آن را در این قسمت قرار دهید.

آیا می دانید که کدام یک از سیستمها و/یا پیکربندیها آسیب پذیر هستند؟

[بله/ خیر] (اگر بله، لطفا آنها را در زیر لیست کنید.)

سیستم:

نسخه سیستم عامل:

اطمینان/ حدس:

آیا شما از ابزار دور زدن آسیب‌پذیری و/ یا بسته های ترمیم آسیب‌پذیری برای این آسیب پذیری آگاهی دارید؟

[بله/ خیر] (اگر شما ابزار دور زدن آسیب‌پذیری دارید یا از وصله ها آگاهی دارید لطفا اطلاعات مربوطه را ذکر کنید.)

آیا اطلاعات دیگری وجود دارد که شما مایل به ذکر آنها باشید؟

۳ سیستم گزارش حادثه مبتنی بر وب

آیا می توان اطلاعات تماس شما را به نهادهای زیر گزارش کرد؟ (در صورت امکان،کنار گزینه مربوطه علامت تیک بزنید.) نهادهای قانونی به فروشندگان محصولات مربوط به حادثه به سایر تیمهای پاسخگویی به حادثه به سایر سایتهای درگیر
آیا می توان رویدادها یا مدارک را به نهادهای زیر ارائه کرد؟ نهادهای قانونی به فروشندگان محصولات مربوط به حادثه به سایر تیمهای پاسخگویی به حادثه به سایر سایتهای درگیر
در صورت امکان، اطلاعات تماس افراد و سازمانهایی که باآنها ارتباط برقرار کرده اید را به طور کامل ذکر کنید.

اطلاعات تماس گزارش دهنده

نام
نام خانوادگی
نام سازمان

عنوان شغلی
آدرس پست الکترونیک
شماره تلفن
از کدام کشور،این گزارش را ارائه می کنید؟(الزامی)
از کدام ناحیه زمانی این گزارش را ارائه می کنید؟(الزامی)
به کدام بخش تجاری وابسته هستید؟(الزامی)
لطفا آدرس کامل پستی خود را بیان کنید.

اطلاعات زیرساختار

لطفا فعالیتهایی که حمله کننده برای انجام آنها تلاش کرده را معین نمایید. افشاء اطلاعات سرقت از منابع فناوری اطلاعات سرقت از دارایی های دیگر تغییر/تخریب اطلاعات کاهش اعتبار هدف حمله سایر
لطفا فعالیتهایی که حمله کننده موفق به انجام آنها شده را معین نمایید. افشاء اطلاعات سرقت از منابع فناوری اطلاعات سرقت از دارایی های دیگر

تغییر/تخریب اطلاعات

کاهش اعتبار هدف حمله

سایر

اطلاعات کلی حادثه

در ابتدا چگونه از وقوع حادثه آگاه شدید؟(الزامی)

اخطار اتوماتیک نرم افزارها (دیوار آتش،نرم افزارهای آنتی ویروس)

مرور اتوماتیک فایلهای رویداد

مرور دستی فایلهای رویداد

شرایط غیرنرمال سیستم (مانند ایجاد وقفه،کند شدن سیستم)

اخطار سازمانهای دیگر

سایر
تکنیک حمله (آسیب پذیریها مورد بهره برداری قرار گرفته اند/استفاده از کدهای استثمارگر)(الزامی) آگاهی از CERT VU،CVE یا شماره Bugtraq ویروس،اسب تروجان،کرم یا کدهای مخرب دیگر حمله انکار سرویس یا انکار سرویس توزیع شده دسترسی بدون اجازه به کامپیوترهای تاثیر دیده،دسترسی در سطح ریشه یا کاربران/دسترسی به وب(تغییر شکل دادن) پویش یا کاوش [۱] سایر

اطلاعات شناسایی[۲]

چگونه فعالیتهای شناسایی را کشف کردید؟ رویدادهای سیستم عامل داده های نظارت بر شبکه نرم افزارهای تشخیص نفوذ نرم افزار دیوار آتش سایر
لطفا هر گونه اخطار، پیغام خطا یا رویداد ثبت شده ای که در توضیح مشکلی که گزارش شده است کمک می کند را کپی کرده و در این قسمت قرار دهید.

[۱] probing

[۲] reconnaissance

لطفا نرم افزار و نسخه مربوط به آن را که در تولید اخطار،پیغام یا ثبت رویداد به کار رفته است ذکر کنید.

اطلاعات فعالیت شبکه

لطفا پروتکلی که درحمله در گیر شده است را تعیین نمایید. TCP UDP ICMP IPsec IP Multicat IPv۶ سایر
لطفا پورت مبدای که در حمله درگیر شده است را معین نمایید. مثال:۲۳،۲۵،۶۰-۹۰،۱۰۲۴
لطفا پورت مقصدی که در حمله درگیر شده است را معین نمایید. مثال:۲۳،۲۵،۶۰-۹۰،۱۰۲۴

اطلاعات تاثیر حمله

تعداد کامپیوترهای میزبانی که تاثیر پذیرفته اند.
تعداد مشتریانی که تاثیر پذیرفته اند.
زمان حمله اول
زمان کشف حمله

آیا حمله پایان یافته است؟ بله خیر
مدت حمله
زمان تقریبی لازم برای ترمیم سیستم
میزان خسارت احتمالی

اطلاعات کامپیوترهای میزبان درگیر

این کامپیوتر میزبان، یک قربانی است یا حمله کننده؟(الزامی) قربانی حمله کننده هر دو
نام کامپیوتر میزبان
آدرس IP
سیستم عامل کامپیوتر میزبان آسیب دیده چیست؟
سطح وصله یا نسخه نرم افزار سیستم عامل چیست؟
وظیفه این کامپیوتر میزبان چیست؟ ایستگاه کاری کاربر سرور وب سرور پست الکترونیک

سرور پروتکل انتقال فایل کنترل کننده دامنه سرور نام دامنه سرور زمان سرور پایگاه داده سرور NFS دیگر سرویس های زیرساختاری
تاثیر واقعی روی کامپیوتر میزبان ناموفق خفیف ویرانگر
تاثیر بالقوه روی کامپیوتر میزبان ناموفق خفیف ویرانگر

اطلاعات اضافی مربوط به حادثه

۴ فرم پاسخ به حادثه

اطلاعات عمومی مربوط به همه انواع حوادث

کمک مورد نیاز

_تماس فوری

_در حال حاضر نیاز به چیزی وجود ندارد.

_پی گیری همه سایتهای آسیب دیده

_تماس با سایتهای حمله کننده

سایتهای درگیر:

نقطه تماس برای بررسی حادثه

نام:

آدرس پست الکترونیک:

نقطه تماس جایگزین برای بررسی حادثه

نام:

آدرس پست الکترونیک:

نوع حادثه

_کد مخرب: ویروس،کرم، اسب تروجان

_پویش

_حمله (نفوذهای موفق/ ناموفق شامل پویش با بسته های حمله)

_حملات انکار سرویس

تاریخ و زمان وقوع حادثه:

خلاصه ای از آنچه اتفاق افتاده است:

نوع اطلاعات، سرویسها یا پروژه هایی که مورد دسترسی قرار گرفته اند

_داده های حساس غیر سری[۳] مانند اطلاعات خصوصی، اموال

_دیگر داده های غیرسری

خسارت وارده

- تعداد سیستمهایی که تاثیر دیده اند:
- ماهیت خسارت:
- زمان قطع سیستم :
- هزینه حادثه:

نام دیگر سایتها که با آنها ارتباط برقرار شده است

نهادهای قانونی:

سایر:

جزئیات کدهای مخرب

مبدا

_دیسکت، سی دی و..

_ضمائم پست الکترونیک

_دانلود نرم افزار

[۳] unclassified

سیستم یا شبکه ای که در ابتدا درگیر شده است:

- آدرس IP یا آدرس زیرشبکه:
- نسخه سیستم عامل:
- نسخه NOS :
- سایر:

سایر سیستمها و شبکه های تاثیر دیده (IP ها و سیستم عاملها):

نوع کد مخرب(در صورت آگاهی از نام کد مخرب، نام هم ذکر شود)

_ویروس:

_اسب تروجان:

_کرم:

_برنامه Joke :

_سایر:

متد عملکرد(برای کدهای مخرب جدید)

_نوع- ماکرو،بوت، مقیم حافظه[۴] ، چند شکلی [۵] ، نهان ،self-encrypting

_payload

_آلوده کردن نرم افزار

_پاک شدن؛تغییر ،رمزنگاری ،حذف فایلها

---

[۴] Memory resident

[۵] Polymorphic

_انتشار از طریق پست الکترونیک

_تغییرات قابل تشخیص

_سایر ویژگیها

جزئیات:

چگونگی تشخیص:

ترمیم(کارهایی که برای بازگرداندن سیستم به حالت عادی انجام شده است)

_نرم افزارهای آنتی ویروس برای عملکرد اتوماتیک تهیه،بهنگام یا نصب شدند.

_سیاستهای جدید برای استفاده از ضمائم پست الکترونیک ایجاد شده است.

_دیوار آتش،روتر و سرورهای پست الکترونیک برای تشخیص و پویش ضمائم، بهنگام شدند.

جزئیات:

توضیحات بیشتر:

جزئیات پویش

مبدا

- آدرس IP
- نام کامپیوتر میزبان
- مکان کامپیوتر نیزبان حمله کننده

_بومی

_خارجی

سیستم یا شبکه ای که در ابتدا درگیر شده است:

- آدرس IP یا آدرس زیرشبکه:
- نسخه سیستم عامل:
- نسخه NOS :

سایر سیستمها و شبکه های تاثیر دیده (IP ها و سیستم عاملها):

متد عملکرد

_پویش/پویش کردن پورتها

_پویش کردن گروهی از آدرسهای IP یا پورتها

_استفاده از ابزار پویش

_هرچیزی که این پویش را منحصر به فرد می کند.

جزئیات:

چگونگی تشخیص

_سایتهای دیگر

_تیم پاسخگویی به حوادث

_فایلهای رویداد

_جمع آوری کننده بسته[۶]

_سیستمهای تشخیص نفوذ

_رفتار غیرعادی

_کاربران

[۶] Packet sniffer

جزئیات:

بخشی از فایل رویداد مربوطه:

توضیحات بیشتر:

جزئیات دسترسی بدون اجازه

مبدا

- آدرس IP
- مکان کامپیوتر میزبان

_بومی

_خارجی

سیستم یا شبکه ای که در ابتدا درگیر شده است:

- آدرس IP یا آدرس زیرشبکه:
- نسخه سیستم عامل:
- نسخه NOS :

سایر سیستمها و شبکه های تاثیر دیده (IP ها و سیستم عاملها):

مسیر حمله

_کلمات عبوری که استراق سمع[۷]، شکسته یا حدس زده شده اند.

_دسترسی به کامپیوترها ی میزبان

_استثمار آسیب پذیریها

[۷] sniffed

_استفاده از ابزار هکر

_مورد هدف قرار گرفتن برنامه کاربردی یا پورت

_مهندسی اجتماعی

جزئیات:

_سطح دسترسی به دست آمده-ریشه / سرپرست،کاربر

متد عملکرد حمله

_پورتها یا پروتکلها مورد حمله واقع شده اند.

_استفاده از ابزار حمله

_نصب ابزارهای هکر مانند rootkit،sniffer،zap ،L۰phtCrack

_به کارگیری یک سرویس مانند IRC

_حمله به بقیه سیستمها یا سایتها

_ایجاد در پشتی

_فایلهایی ایجاد، کپی، حذف، تغییر یا تروجان شده اند.

_ایجاد حساب کاربری و استفاده از کلمات عبور

_رویه های غیرمعمول درحال اجرا هستند.

_سایر

جزئیات:

چگونگی تشخیص

_سایتهای دیگر

_تیم پاسخگویی به حوادث

_فایلهای رویداد

_جمع آوری کننده بسته

_سیستمهای تشخیص نفوذ

_رفتار غیرعادی

_کاربران

TCP Wrapper_

Tripwire_

_سایر

جزئیات:

بخشی از فایل رویداد مربوطه:

توضیحات بیشتر:

ترمیم(کارهایی که برای بازگرداندن سیستم به حالت عادی انجام شده است)

_استفاده از وصله

_اجرای پویشگرها

_نصب نرم افزارهای امنیتی

_حذف سرویسها و برنامه های کاربردی غیرضروری

_نصب مجدد سیستم عامل

_بازگرداندن سیستمها به حالت عادی با استفاده از نسخه پشتیبان

_انتقال برنامه های کاربردی به یک سیستم دیگر

_افزایش حافظه یا فضای دیسک

_قرار دادن سیستم پشت یک مسیریاب فیلترینگ یا دیوار آتش

_فایلهای مخفی تشخیص و حذف شدند.

_نرم افزارهای تروجان تشخیص و حذف شدند.

_برای نظارت بر رفتار هکر تغییری در سیستم داده نشده است.

_سایر

جزئیات:

توضیحات بیشتر:

جزئیات حوادث انکار سرویس

مبدا

- آدرس IP
- مکان کامپیوتر میزبان

_بومی

_خارجی

سیستم یا شبکه ای که در ابتدا درگیر شده است:

- آدرس IP یا آدرس زیرشبکه:
- نسخه سیستم عامل:

- نسخه NOS :
- سایر:

سایر سیستمها و شبکه های تاثیر دیده (IP ها و سیستم عاملها):

متد عملکرد

_استفاده از ابزار

_سیلاب بسته

_بسته های مخرب

_ جعل IP

_حمله به پورتها

_هرجیزی که این حادثه را منحصر به فرد می کند.

جزئیات:

ترمیم(کارهایی که برای حفاظت از سیستم انجام شده است):

_ انتقال برنامه های کاربردی به یک سیستم دیگر

_ افزایش حافظه یا فضای دیسک

_نصب shadow server

_سایر

جزئیات:

بخشی از فایل رویداد مربوطه:

توضیحات اضافی:

۵ فرم گزارش نهایی پس از رفع حادثه

تاریخ گزارش:
گزارش شده توسط نام: سمت: شماره تلفن: آدرس پست الکترونیک:
جزئیات حادثه
تاریخ حادثه:
نوع حادثه:
نام سیستم و توضیح:
خلاصه ای از حادثه:

ترتیب حوادث:

تاریخ/ ساعت حادثه

اعمال انجام شده و نتایج:

وضعیت جاری سیستم:

افراد درگیر:

نام سمت شماره تلفن پست الکترونیک

سایتها/سیستمهای آسیب دیده:

خسارت (شامل قطع سرویس)

هزینه(شامل خسارت ناشی از حادثه و هزینه ترمیم)

اعمال پیشنهادی برای جلوگیری از وقوع مجدد:
توضیحات دیگر:
مطالب آموخته شده:

۶ منابع و مراجع

www.cert.org/reporting/incident_form.txt

www.cert.org/archive/pdf/۰۳tr۰۰۱.pdf

www.ogcio.gov.hk/eng/prodev/download/g۵۴_pub.pdf

https://irf.cc.cert.org