دستورالعمل تکمیل فرم گزارش رخداد

دستورالعمل تکمیل فرم گزارش رخداد

کلیات

کلیه ذی‌نفعان و موجودیت‌های درون‌سازمانی و برون‌سازمانی ذکرشده در سند تدوین مدل ارتباطی می‌توانند اقدام به پر کردن فرم گزارش رخداد نمایند. فرم‌های گزارش رخداد تکمیل‌شده، توسط شخص تکمیل‌کننده فرم طبقه‌بندی گردیده و مسئولیت حفظ آن‌ها بر عهده مرکز MCI-CERT خواهد بود. فرم‌های گزارش رخداد پس از تکمیل در پایگاه دانش مرکز ثبت و نگهداری می‌گردند. فرم گزارش رخداد پس از تکمیل در اختیار کارشناسان گروه دریافت و تریاژ قرار می‌گیرند. یک رونوشت از فرم گزارش رخداد تکمیلی جهت آرشیو برای کارشناسان گروه مستندسازی و انتشار ارسال می‌گردد. همچنین رونوشت‌هایی از این فرم به مدیرکل ایمنی شبکه و رئیس اداره واکنش به رخداد اداره واکنش به رخداد ارسال می‌گردد. این فرم برای ثبت اطلاعات مربوط به رخدادهای کشف‌شده تکمیل و تنظیم می‌گردد. فیلدهایی از فرم که با (*) نشان‌گذاری شده است، بیان‌کننده اجباری بودن پر کردن این فیلد می‌باشد.

نحوه تکمیل فرم گزارش رخداد

- **اطلاعات گزارش‌دهنده**

اطلاعات گزارش دهنده	
نام و نام خانوادگی:	سازمان/ اداره:
سمت:	ایمیل:
آدرس پستی:	
کد پستی:	تلفن:
موبایل:	فکس:

- **نام و نام خانوادگی:** نام و نام خانوادگی شخص گزارش‌دهنده رخداد در این بخش درج می‌گردد.
- **سازمان/اداره:** نام سازمان/اداره‌ای که شخص گزارش‌دهنده رخداد در آن مشغول به کار است، تعیین می‌گردد.
- **سمت:** بیان‌کننده سمت و عنوان شغلی گزارش‌دهنده است.
- **ایمیل:** بیان‌کننده آدرس ایمیل (یا پست الکترونیکی) شخص گزارش‌دهنده است. برای واردکردن چندین ایمیل می‌توان آن‌ها را با استفاده از **";"** از هم جدا کرد.
- **آدرس پستی:** آدرس پستی شخص گزارش‌دهنده از سمت راست به چپ و بر اساس قالب [استان]، [شهر]، [خیابان]، [کوچه]، [پلاک]، [طبقه] و [واحد/اتاق] در این بخش درج می‌گردد.

- **کدپستی:** کدپستی شخص گزارش‌دهنده بر اساس قالب [کدپستی ده‌رقمی] در این بخش درج می‌گردد (برای مثال ۱۲۳۴۵-۶۷۸۹۰).**تلفن:** شماره تلفن داخل ایران شخص گزارش‌دهنده از سمت چپ به راست و بر اساس قالب [شماره داخلی]-[شماره محلی]-[کد کشور] تکمیل می‌گردد. (برای مثال به‌صورت ۰۰۹۸-۱۲۳۴-۵۶۷۸)
- **موبایل:** شماره موبایل متعلق به شخص گزارش‌دهنده از سمت چپ به راست و بر اساس قالب [شماره موبایل]-[کد کشور] تکمیل می‌گردد. (برای مثال به‌صورت ۰۰۹۸-۹۱۲۳۴۵۶۷۸۹)
- **فکس:** شماره فکس مربوط به شخص گزارش‌دهنده از سمت چپ به راست و بر اساس قالب [شماره داخلی]-[شماره محلی]-[کد کشور] تکمیل می‌گردد. (برای مثال به‌صورت ۰۰۹۸-۱۲۳۴-۵۶۷۸)

- **اطلاعات رخداد**

اطلاعات رخداد
عنوان رخداد (*):
زمان گزارش رخداد (*):
محدودیت انتشار (*): ☐ عمومی ☐ افرادی که نیاز دارند ☐ خصوصی ☐ پیش‌فرض ☐ نامشخص

- **عنوان رخداد:** در این بخش عنوان رخداد به وقوع پیوسته درج می‌گردد.
- **زمان گزارش رخداد:** شامل زمان و تاریخی است که رخداد گزارش می‌گردد. این مقدار می‌بایست از سمت چپ به راست و بر اساس قالب [ثانیه]:[دقیقه]:[ساعت به‌صورت ۲۴ ساعته]-[روز به‌صورت دورقمی]/[ماه به‌صورت دورقمی]/[سال هجری شمسی به‌صورت چهاررقمی] درج گردد. (برای مثال ۰۱-۲۰:۱۷/۰۱/۱۳۹۴)
- **محدودیت انتشار:** بیان‌کننده میزان محدودیت برای انتشار اطلاعات مندرج در فرم گزارش رخداد می‌باشد که برحسب محتوای فرم، مقادیر زیر برای این ویژگی قابل انتخاب است.
  - ⊡ عموم: هیچ محدودیتی برای انتشار اطلاعات به‌طور عام وجود ندارد.
  - ⊡ نیاز به دانش[1]: اطلاعات ممکن است بین بخش‌هایی که با رخداد درگیر می‌باشند، به اشتراک گذاشته شود.
  - ⊡ خصوصی: اطلاعات قابل اشتراک‌گذاری نمی‌باشد.
  - ⊡ پیش‌فرض: اطلاعات می‌توانند بر اساس خط‌مشی افشای اطلاعات از پیش تعیین‌شده، انتشار یابند.

[1] Need-to-know

⊡ نامشخص: درصورتی‌که شخص گزارش‌دهنده از میزان محدودیت مربوط به انتشار اطلاعات مندرج در فرم گزارش رخداد آگاهی نداشته باشد، می‌بایست این گزینه توسط وی انتخاب گردد.

- **وضعیت**

وضعیت (*)					
در حال وقوع	☐	به وقوع پیوسته (غیرفعال)	☐	وقوع مجدد رخداد حل نشده	☐

- **وضعیت:** بسته به وضعیت رخداد کشف‌شده، یکی از وضعیت‌های در حال وقوع، به وقوع پیوسته و وقوع مجدد رخداد حل‌نشده انتخاب می‌گردد.

- **اطلاعات زمانی**

اطلاعات زمانی
زمان شروع رخداد:
زمان خاتمه رخداد:
زمان تشخیص رخداد (*):

- **زمان شروع رخداد:** بیان‌کننده زمانی است که رخداد آغاز می‌گردد. قالب درج این مقدار به‌صورت [ثانیه]:[دقیقه]:[ساعت به‌صورت ۲۴ ساعته]-[روز به‌صورت دورقمی]/[ماه به‌صورت دورقمی]/[سال هجری شمسی به‌صورت چهاررقمی] می‌باشد. (برای مثال ۱۳۹۴/۰۱/۰۱-۱۷:۲۰)
- **زمان خاتمه رخداد:** بیان‌کننده زمانی است که رخداد خاتمه می‌یابد. قالب درج این مقدار به‌صورت [ثانیه]:[دقیقه]:[ساعت به‌صورت ۲۴ ساعته]-[روز به‌صورت دورقمی]/[ماه به‌صورت دورقمی]/[سال هجری شمسی به‌صورت چهاررقمی] می‌باشد. (برای مثال ۱۳۹۴/۰۱/۰۱-۱۷:۲۰)
- **زمان تشخیص رخداد:** بیان‌کننده زمانی است که رخداد برای نخستین بار تشخیص داده می‌شود. قالب درج این مقدار به‌صورت [ثانیه]:[[دقیقه]:[ساعت به‌صورت ۲۴ ساعته]-[روز به‌صورت دورقمی]/[ماه به‌صورت دورقمی]/[سال هجری شمسی به‌صورت چهاررقمی] می‌باشد. (برای مثال ۱۳۹۴/۰۱/۱۷:۲۰-۰۱)

- **نوع رخداد**

نوع رخداد (*)

ممانعت از سرویس	☐	اطلاعات به مخاطره افتاده	☐	دارایی‌های به مخاطره افتاده	☐		
فعالیت‌های غیرقانونی	☐	نفوذ داخلی	☐	نفوذ خارجی	☐		
جمع‌آوری اطلاعات	☐	بدافزار	☐	ایمیل	☐		
تخطی از خط‌مشی	☐	سایر	☐				

- **نوع رخداد:** نوع رخداد کشف‌شده بر اساس یکی از موارد ذکرشده در این بخش، تعیین می‌گردد.

سطح تأثیر

سطح تاثیر

سرویس/ سامانه تحت تاثیر (*):

تعداد تقریبی کاربران تحت تاثیر (*):

- **سرویس/سامانه‌های تحت تأثیر:** لیستی از مشخصات سرویس/سامانه‌هایی که با بروز رخداد گزارش‌شده تحت تأثیر قرار گرفته‌اند، در این بخش ذکر می‌گردد.
- **تعداد تقریبی کاربران تحت تأثیر:** تعداد تقریبی افرادی که تحت تأثیر رخداد گزارش‌شده می‌باشند، تعیین می‌گردد.

فوریت

فوریت (*)

آیا اطلاعات طبقه‌بندی شده تحت تاثیر قرار گرفته است؟	بلی ☐	خیر ☐
آیا رخداد در حال گسترش می‌باشد؟	بلی ☐	خیر ☐

- **فوریت:** فوریت رخداد به وقوع پیوسته با پاسخ به دو سؤال مطرح‌شده در این بخش، تعیین می‌گردد.

اطلاعات تکمیلی رخداد

اطلاعات تکمیلی رخداد (*)

شرح رخداد سخت‌افزاری:

شرح رخداد نرم‌افزاری:

شرح رخداد فرآیندی:

سایر موارد:

نحوه تشخیص رخداد (*):

- **شرح رخداد سخت‌افزاری:** یک توصیف متنی و فاقد ساختار خاص در خصوص رخداد سخت‌افزاری واقع‌شده بیان می‌گردد.

- **شرح رخداد نرم‌افزاری:** یک توصیف متنی و فاقد ساختار خاص در خصوص رخداد نرم‌افزاری واقع‌شده بیان می‌گردد.
- **شرح رخداد فرآیندی:** یک توصیف متنی و فاقد ساختار خاص در خصوص رخداد فرآیندی واقع‌شده بیان می‌گردد.
- **سایر موارد:** یک توصیف متنی و فاقد ساختار خاص در خصوص سایر رخدادهای واقع‌شده بیان می‌گردد.
- **نحوه تشخیص رخداد:** در این بخش یک توصیف متنی و فاقد ساختار خاص در مورد تکنیک‌ها، متدها و همچنین چگونگی تشخیص رخداد گزارش‌شده بیان می‌گردد.

◆ **اطلاعات سیستم‌های تحت تأثیر (هدف)**

اطلاعات سیستم‌های تحت تاثیر (هدف)

نام میزبان یا آدرس‌های IP (*):

کارکرد سیستم (*):

سیستم عامل (*):

سایر توضیحات:

- **نام میزبان یا آدرس‌های IP:** در این بخش مشخصات مربوط به سیستم میزبان از قبیل نام یا آدرس IP، درج می‌گردد. به‌منظور درج آدرس IP می‌بایست از استاندارد درج آدرس IP نسخه ۴ به‌صورت دهدهی (مانند ۱۹۲,۱۶۸,۱,۱) و یا نسخه ۶ در مبنای ۱۶ (مانند 2001:0db8:85a3:0042:1000:8a2e:0370:7334) استفاده گردد.
- **کارکرد سیستم:** در این بخش کارکرد سیستمی که تحت تأثیر رخداد گزارش‌شده قرارگرفته است، بیان می‌گردد.
- **سیستم‌عامل:** نام سیستم‌عامل موجود بر روی سیستم‌های تحت تأثیر تعیین و درج می‌گردد.

- **سایر توضیحات:** سایر اطلاعات مربوط به سیستم‌های تحت تأثیر در صورت معلوم بودن از قبیل پروتکل‌های مناسب استفاده‌شده در حمله، مشخصات مربوط به آنتی‌ویروس‌های نصب‌شده بر روی سیستم‌های تحت تأثیر، پورت‌هایی از سیستم تحت تأثیر و سیستم حمله‌کننده که در حمله درگیر می‌باشند، آدرس IP حمله‌کننده و غیره بیان می‌گردد. به‌منظور درج آدرس IP می‌بایست از استاندارد درج آدرس IP نسخه ۴ به‌صورت ده‌دهی (مانند ۱۹۲,۱۶۸,۱,۱) و یا نسخه ۶ در مبنای ۱۶ (مانند 2001:0db8:85a3:0042:1000:8a2e:0370:7334) استفاده گردد.

- **اطلاعات منشأ رخداد**

اطلاعات منشاء رخداد

نام میزبان یا آدرس‌های IP:

سایر توضیحات:

- **نام میزبان یا آدرس IP:** در این بخش مشخصات مربوط به سیستمی که رخداد از آن منشأ گرفته از قبیل نام یا آدرس IP، درج می‌گردد. به‌منظور درج آدرس IP می‌بایست از استاندارد درج آدرس IP نسخه ۴ به‌صورت ده‌دهی (مانند ۱۹۲,۱۶۸,۱,۱) و یا نسخه ۶ در مبنای ۱۶ (مانند 2001:0db8:85a3:0042:1000:8a2e:0370:7334) استفاده گردد.
- **سایر توضیحات:** سایر اطلاعات مربوط به سیستم‌های منشأ رخداد در صورت معلوم بودن از قبیل پورت‌هایی از سیستم حمله‌کننده که در حمله درگیر می‌باشند، آدرس IP حمله‌کننده و غیره بیان می‌گردد. به‌منظور درج آدرس IP می‌بایست از استاندارد درج آدرس IP نسخه ۴ به‌صورت ده‌دهی (مانند ۱۹۲,۱۶۸,۱,۱) و یا نسخه ۶ در مبنای ۱۶ (مانند 2001:0db8:85a3:0042:1000:8a2e:0370:7334) استفاده گردد.