آزمایشگاه آپا

آگاهی‌رسانی، پشتیبانی و امداد در

حوزه امنیت سیستم‌عامل

دانشگاه صنعتی امیرکبیر

(با حمایت مرکز تحقیقات مخابرات ایران)

گروه مدیریت

الویت دهی به آسیب پذیریها با استفاده از CVSS

FC_۸۷_۰۷_۰۱

تاریخ: ۸۷/۰۷

مشخصات سند			
نام سند:			
کد فایل	**آخرین نسخه**	**تاریخ آخرین بازبینی**	**گروه**
FC_۸۷_۰۷_۰۱	۱،۱	۸۷/۰۹/۰۵	مدیریت

سابقه سندها			
نسخه	**تاریخ تنظیم**	**تنظیم‌کننده**	**توضیحات**
۱،۰	۸۷/۰۷/۰۷	خدیجه محمدزاده	ایجاد

چکیده

CVSS یک روش برای امتیازدهی آسیب پذیریها به منظور تعیین الویت آنها است این روش توسط FIRST[1] ارائه شده است.در این گزارش معیارهای و معادلات مورد استفاده در روش CVSS آمده است.

[1] Forum for Incident Response and Security Teams

فهرست مطالب

۱ مقدمه..... ۱

۲ سیستم امتیازدهی آسیب‌پذیری چیست؟ ۱

۳ معیارهای سیستم امتیازدهی آسیب‌پذیری متعارف..... ۲

۳-۱ معیارهای پایه ای..... ۲

۳-۱-۱ بردار دسترسی (AV) ۲

۳-۱-۲ پیچیدگی دسترسی (AC)..... ۳

۳-۱-۳ تصدیق اصالت (AU) ۴

۳-۱-۴ تاثیر بر محرمانگی..... ۴

۳-۱-۵ تاثیر جامعیت (I) ۵

۳-۱-۶ تاثیر در دسترس پذیری (A)..... ۵

۳-۲ معیارهای موقتی ۶

۳-۲-۱ "قابلیت بهره برداری" (E)..... ۶

۳-۲-۲ سطح ترمیم (RL) ۷

۳-۲-۳ اطمینان از گزارش (RC) ۸

۳-۳ معیارهای محیطی..... ۹

۳-۳-۱ خسارت بالقوه (CDP) ۹

۳-۳-۲ توزیع هدف (TD)..... ۱۰

۳-۳-۳ نیازهای امنیتی (CR,IR,AR)..... ۱۱

۴ بردارهای پایه،موقتی و محیطی..... ۱۲

۵ امتیازدهی..... ۱۲

۵-۱ نکات عمومی..... ۱۳

۵-۲ معیارهای پایه..... ۱۳

۵-۲-۱ بردار دسترسی..... ۱۳

۵-۲-۲ تصدیق اصالت..... ۱۴

۵-۲-۳ تاثیرهای محرمانگی،جامعیت و در دسترس پذیری..... ۱۴

۵-۲-۴ معادله پایه..... ۱۴

۵-۲-۵ معادله موقتی..... ۱۶

۵-۲-۶ معادله محیطی..... ۱۷

۶ منابع و مراجع ۲۰

فهرست جداول

جدول ۱- امتیاز دهی به بردار دسترسی ۲

جدول۲-امتیازدهی پیچیدگی دسترسی ۳

جدول ۳-امتیاز دهی به تصدیق اصالت ۴

جدول۴-امتیاز دهی به تاثیر بر محرمانگی ۴

جدول ۵-امتیاز دهی به تاثیر جامعیت ۵

جدول۶-امتیاز دهی به در دسترس پذیری ۶

جدول ۷-امتیاز دهی به قابلیت بهره برداری ۶

جدول ۸-امتیاز دهی به سطح ترمیم ۷

جدول ۹-امتیاز دهی به اطمینان از گزارش ۸

جدول۱۰-امتیاز دهی به میزان خسارت بالقوه ۹

جدول ۱۱-امتیاز دهی به توزیع هدف ۱۰

جدول۱۲-امتیاز دهی به نیازهای امنیتی ۱۱

جدول ۱۳-بردارهای پایه،موقتی و محیطی ۱۲

۱ مقدمه

برای بررسی آسیب‌پذیریها باید آن‌ها را الویت دهی کرده و آن‌هایی که ریسک بیشتری تولید می‌کنند را ابتدا مورد بررسی قرار داد. زمانی که چندین آسیب‌پذیری وجود دارند که با استفاده از روشهای مختلفی امتیاز دهی شده‌اند نمی‌توان الویت دهی مناسبی انجام داد. "*سیستم امتیاز دهی آسیب‌پذیری متعارف*"[۲] (CVSS) این مشکل را برطرف ساخته است. با استفاده از سیستم امتیازدهی آسیب‌پذیری متعارف، امتیازی که به هر یک از آسیب‌پذیریها اختصاص داده می‌شود نشانگر ریسک واقعی آن آسیب‌پذیری برای سازمان است و با استفاده از آن می‌توان الویت دهی را انجام داد.

۲ سیستم امتیازدهی آسیب‌پذیری چیست؟

سیستم امتیازدهی آسیب‌پذیری متعارف از سه گروه معیار اساسی، موقتی و محیطی تشکیل شده است.هر یک از این گروهها نیز از مجموعه‌ای از معیارها تشکیل شده‌اند.

معیارهای پایه‌ای: این معیارها ویژگیهای اصلی و پایه‌ای یک آسیب‌پذیری هستند که در طول زمان ثابت بوده و به محیط کاربر بستگی ندارند.

معیارهای موقتی: این معیارها با گذشت زمان تغییر کرده ولی بین محیطهای کاربری مختلف یکسان هستند.

معیارهای محیطی: این معیارها به یک محیط خاص کاربری مربوط بوده و منحصر به آن محیط هستند.

زمانی که به معیارهای پایه ای مقادیر مناسب اختصاص داده شد معادله پایه ای مقداری بین ۰ تا ۱۰ خواهد داشت و یک بردار ایجاد خواهد نمود. بردار که یک رشته متنی است شامل مقادیر اختصاص داده شده به هر یک از معیارها است. بنابراین هر کس می‌تواند به آسانی بفهمد که به هر یک از معیارها چه مقادیری اختصاص داده شده است و در صورت لزوم اعتبار آن را تایید کند.

استفاده از معیارهای موقتی و محیطی اختیاری است ولی می‌توان با تخصیص مقادیر مناسب به این معیارها امتیاز پایه را پالایش کرد. استفاده از معیارهای موقتی و محیطی ریسکی که آسیب‌پذیری در معرض محیط کاربر قرار می‌دهد را با دقت بیشتری منعکس می‌کند اما استفاده از این معیارها الزامی نیست و با توجه به هدف، ممکن است استفاده از امتیاز پایه کافی باشد.

اگر از امتیاز محیطی استفاده شود معادله محیطی معیارهای موقتی را با امتیاز پایه ترکیب کرده و یک امتیاز موقتی بین ۰ تا ۱۰ تولید خواهد کرد به طور مشابه اگر از امتیاز محیطی استفاده شود معادله محیطی، معیارهای محیطی را با امتیاز موقتی ترکیب کرده و یک امتیاز محیطی بین ۰ تا ۱۰ تولید خواهد کرد.

---

[۲] Common Vulnerability Scoring System

۳ معیارهای سیستم امتیازدهی آسیب‌پذیری متعارف

۳-۱ معیارهای پایه ای

این بخش شامل معیارهایی می‌شود که با گذشت زمان ثابت مانده و بین محیطهای کاربری مختلف یکسان هستند. بردارهای دسترسی، پیچیدگی دسترسی و معیارهای تصدیق اصالت، چگونگی دسترسی به آسیب‌پذیری و شرطهای مورد نیاز برای استثمار آسیب‌پذیری را بررسی می‌کنند. تاثیر یک آسیب‌پذیری با سه معیار جامعیت، محرمانگی و در دسترس‌پذیری سنجیده می‌شود این سه معیار نشان می‌دهند که چگونه یک آسیب‌پذیری، اگر بتوان از آن بهره‌برداری کرد، تاثیر مستقیم بر ساختار فناوری اطلاعات خواهد گذاشت.

۳-۱-۱ بردار دسترسی[۳] (AV)

این معیار چگونگی استثمار آسیب‌پذیری را منعکس می‌کند مقادیر ممکن برای این معیار در جدول زیر لیست شده‌اند اگر حمله‌کننده بتواند از راه دور به یک کامپیوتر میزبان حمله کند امتیاز بیشتری به آن تعلق خواهد گرفت.

جدول ۱- امتیاز دهی به بردار دسترسی

مقدار معیار	توضیح
محلی(L)	در آسیب‌پذیری که فقط با دسترسی محلی قابل بهره‌برداری است حمله‌کننده به دسترسی فیزیکی به سیستم آسیب پذیر یا به یک حساب محلی نیاز دارد یک مثال از آسب‌پذیریهای قابل بهره‌برداری محلی، آسیب‌پذیری *افزایش مجوز محلی*[۴] (sudo) است.
شبکه مجاور(A)	حمله‌کننده باید به دامنه تصادم[۵] یا انتشار[۶] نرم‌افزار آسیب پذیر دسترسی داشته باشد به عنوان مثال می‌توان به IEEE ۸۰۲،۱۱ اشاره کرد.
شبکه(N)	در آسیب‌پذیری قابل بهره‌برداری از راه شبکه، نرم‌افزار آسیب پذیر در پشته شبکه قرار می گیرد و حمله‌کننده به دسترسی به شبکه محلی یا دسترسی محلی نیازی ندارد این آسیب‌پذیریها قابل بهره‌برداری از راه دور نامیده می‌شوند. نمونه‌ای از این حمله سرریز بافر فراخوانی روال از دور[۷] است.

[۳] Access Vector

[۴] local privilege escalation

[۵] collision domain

[۶] broadcast

[۷] RPC buffer overflow

۳-۱-۲ پیچیدگی دسترسی [۸](AC)

این معیار پیچیدگی بهره‌برداری از آسیب‌پذیری، پس از به دست آوردن دسترسی، را اندازه گیری می‌کند. به عنوان مثال در سرریز بافر، زمانی که سیستم هدف مکانیابی شد حمله‌کننده می‌تواند یک کد استثمارگر را روی آن اجرا کند در حالی که بقیه آسیب‌پذیریها به گامهای بیشتری برای بهره‌برداری نیاز دارند به عنوان مثال یک آسیب‌پذیری در سرویس گیرنده پست الکترونیکی پس از دانلود و باز کردن ضمائم آلوده قابل بهره‌برداری است .مقادیر ممکن برای تخصیص به این معیارها در جدول زیر لیست شده‌اند. هر چه پیچیدگی کمتر باشد امتیاز بیشتری به آن تعلق خواهد گرفت.

جدول ۲-امتیازدهی پیچیدگی دسترسی

مقدار معیار	توضیح
زیاد (H)	شرایط دسترسی تخصصی لازم است به عنوان مثال: • در بسیاری از پیکربندیها بخش حمله‌کننده باید مجوز را افزایش دهد یا علاوه بر سیستم مهاجم، سیستم‌های دیگری را نیز جعل کند (سرقت نام دامنه [۹]) • پیکربندیهای آسیب پذیر به ندرت دیده می‌شوند. • حمله با متدهای مهندسی اجتماعی[۱۰] انجام می‌شود که به آسانی توسط افراد مطلع شناسایی می‌شود.به عنوان مثال قربانی باید چندین عمل مشکوک و غیر معمول را انجام دهد.
متوسط (M)	شرایط دسترسی تا حدی تخصصی هستند در زیر نمونه‌هایی آورده شده است: • بخش مهاجم به گروهی از سیستم‌ها یا کاربران محدود شده است. • قبل از انجام یک حمله موفق باید اطلاعاتی جمع‌آوری شود. • پیکربندی تاثیر یافته، پیش فرض ندارد و معمولا تنظیم نمی‌شود(آسیب‌پذیری در زمانی که سرور با استفاده از یک رویه خاص، حساب کاربر را تصدیق اصالت می‌کند وجود دارد ولی وقتی با استفاده از یک رویه دیگر تصدیق اصالت انجام می‌شود آسیب‌پذیری وجود ندارد) .
کم (L)	شرایط دسترسی تخصصی وجود ندارد به عنوان مثال: • پیکربندی تاثیر دیده در همه جا موجود است یا به صورت پیش فرض وجود دارد. • حمله را می‌توان به صورت دستی انجام داد و به مهارت کمی نیاز دارد هم‌چنین به جمع‌آوری اطلاعات اضافی چندانی نیاز ندارد.

[۸] Access Complexity

[۹] DNS hijacking

[۱۰] Social engineering

۳-۱-۳ تصدیق اصالت[۱۱] (AU)

این معیار تعداد دفعاتی که حمله‌کننده باید پیش از دسترسی به هدف و بهره‌برداری از آن تصدیق اصالت کند را در نظر می‌گیرد و به پیچیدگی فرآیند تصدیق اصالت توجهی ندارد و فقط تعداد دفعاتی که حمله‌کننده قبل از بهره‌برداری از آسیب‌پذیری باید کلمه عبور و شناسه کاربری را وارد کند اندازه می‌گیرد .مقادیر ممکن برای این معیار در جدول زیر ذکر شده است.هر چه تعداد تصدیق اصالت کمتری مورد نیاز باشد امتیاز بیشتری تعلق خواهد گرفت.

جدول ۳-امتیاز دهی به تصدیق اصالت

مقدار معیار	توضیح
متعدد (M)	حمله‌کننده برای بهره‌برداری از آسیب‌پذیری باید دوبار یا بیشتر تصدیق اصالت کند. (حتی اگر از همان شناسه کاربر و کلمه عبور استفاده شود)
واحد (S)	یک تصدیق اصالت برای دسترسی و بهره‌برداری از آسیب‌پذیری نیاز ست.
هیچ (N)	برای بهره‌برداری از آسیب‌پذیری به تصدیق اصالت نیازی نیست.

۳-۱-۴ تاثیر بر محرمانگی[۱۲]

این معیار اثر بهره‌برداری موفق از یک آسیب‌پذیری بر محرمانگی را اندازه‌گیری می‌کند .منظور از محرمانگی محدود کردن دسترسی به اطلاعات و افشاء آن‌ها به کاربران مجاز و جلوگیری از دسترسی یا افشاء اطلاعات به کاربران غیرمجاز است.

جدول ۴-امتیاز دهی به تاثیر بر محرمانگی

مقدار معیار	توضیح
هیچ (N)	هیچ تاثیری روی محرمانگی سیستم ندارد.

[۱۱] Authentication

[۱۲] confidentiality

ناقص[۱۳](P)	افشاء اطلاعات قابل توجهی وجود دارد و دسترسی به برخی فایل‌های سیستم امکانپذیر است ولی حمله‌کننده کنترلی روی چیزی که به دست می آورد ندارد یا حوزه زیان، محدود شده است به عنوان مثال می‌توان به آسیب‌پذیری که فقط می‌تواند جداول خاصی از پایگاه داده را افشاء سازد اشاره کرد.
کامل(C)	همه فایل‌های سیستم افشاء شده‌اند و حمله‌کننده می‌تواند همه داده‌های سیستم را بخواند.

۳-۱-۵ تاثیر جامعیت[۱۴] (I)

این معیار اثر یک بهره‌برداری موفق بر جامعیت را اندازه می‌گیرد. منظور از جامعیت، قابلیت اعتماد و تضمین صحت اطلاعات است. مقادیر ممکن برای این معیار در جدول زیر ذکر شده‌اند.هرچه تاثیر روی جامعیت بیشتر باشد امتیاز بیشتری تعلق خواهد گرفت.

جدول ۵-امتیاز دهی به تاثیر جامعیت

مقدار معیار	توضیح
هیچ (N)	تاثیری روی جامعیت اطلاعات ندارد.
ناقص(P)	تغییر برخی فایل‌های سیستم یا اطلاعات ممکن است ولی حمله‌کننده کنترلی روی آنچه می‌تواند تغییر داده شود ندارد یا حوزه ای که حمله‌کننده می‌تواند آن را تحت تاثیر قرار دهد محدود است.
کامل(C)	حمله‌کننده می‌تواند هر فایلی در سیستم مقصد را تغییر دهد.

۳-۱-۶ تاثیر در دسترس پذیری[۱۵] (A)

این معیار اثر یک بهره‌برداری موفق از آسیب‌پذیری را بر دسترس پذیری اندازه گیری می‌کند. حملاتی که پهنای باند شبکه، توان پردازنده و فضای دیسک را مصرف می‌کنند بر در دسترس پذیری سیستم تاثیر می‌گذارند. مقادیر ممکن برای این معیار در جدول زیر ذکر شده است.هر چه تاثیر در دسترس‌پذیری بیشتر باشد امتیاز بیشتری تعلق خواهد گرفت.

---

[۱۳] partial

[۱۴] Integrity

[۱۵] Availability

جدول ۶-امتیاز دهی به در دسترس پذیری

مقدار معیار	توضیح
هیچ (N)	تاثیری بر دسترس پذیری سیستم ندارد.
ناقص(P)	در دسترسی به منابع وقفه هایی وجود دارد یا کارآیی کاهش یافته است به عنوان مثال می‌توان به یک حمله سیلابی[۱۶] متکی بر شبکه که تعداد ارتباطات موفق به یک سرویس اینترنتی را محدود می‌کند اشاره کرد.
کامل(C)	همه منابع تاثیریافته قطع می‌شوند و حمله‌کننده سیستم را کاملا غیرقابل دسترس می‌کند.

۳-۲ معیارهای موقتی

تهدید ناشی از یک آسیب‌پذیری ممکن است با گذشت زمان تغییر کند. سه معیار که توسط سیستم امتیازدهی آسیب‌پذیری متعارف در این زمینه ارائه شدند عبارتند از: تصدیق جزئیات فنی یک آسیب‌پذیری، وضعیت ترمیم آسیب‌پذیری و در دسترس‌پذیری کدهای استثمارگر یا تکنیکها. از آنجایی که معیارهای موقتی، اختیاری هستند هر یک از آن‌ها یک مقدار معیار برای اینکه تاثیری روی امتیاز نهایی نداشته باشند دارند. این مقدار زمانی استفاده می‌شود که کاربر احساس کند یک معیار خاص نمی‌تواند مورد استفاده قرار بگیرد و می خواهد از روی آن عبور کند.

۳-۲-۱ *"قابلیت بهره برداری"* [۱۷] (E)

این معیار وضعیت جاری تکنیکها یا کدهای استثمارگر را بیان می‌کند. دسترسی عمومی به کدهای استثمارگر که استفاده از آن‌ها آسان است تعداد حمله کننده‌های بالقوه را با دربرگرفتن حمله کننده‌های غیرماهر افزایش می‌دهد و در نتیجه شدت آسیب‌پذیری افزایش می‌یابد.

مقادیر ممکن برای این معیار در جدول زیر ذکر شده‌اند هرچه آسانتر بتوان از یک آسیب‌پذیری بهره‌برداری کرد امتیاز بیشتری به آن تعلق خواهد گرفت.

جدول۷-امتیاز دهی به قابلیت بهره برداری

مقدار معیار	توضیح

[۱۶] Flood attack

[۱۷] Exploitability

اثبات نشده (U)	کد استثمارگری در دسترس نیست یا استثمار در کل در حد تئوری است.
اثبات مفهوم[۱۸] (POC)	کد استثمارگر که درستی مفهوم آن اثبات شده و برای بسیاری از سیستم‌ها عملی نیست در دسترس است. کد یا تکنیک در همه موقعیتها عملی نیست و ممکن است به تغییرات اساسی توسط حمله‌کننده نیاز داشته باشد.
در حال کار[۱۹] (F)	کد استثمارگر در دسترس است و در بسیاری از موقعیتهایی که آسیب‌پذیری وجود دارد کار می‌کند.
زیاد (H)	آسیب‌پذیری از طریق *کدهای مستقل سیار*[۲۰] قابل بهره‌برداری است یا به گونه‌ای است که به استثمار نیاز ندارد (فعال شدن به طور دستی). جزئیات به نحوگسترده‌ای در دسترس است. کد در هر حالتی کار می‌کند یا از طریق یک عامل مستقل سیار تحویل داده می‌شود. (مانند کرم یا ویروس)
تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار روی امتیاز نهایی تاثیری نخواهد گذاشت.

۳-۲-۲ سطح ترمیم[۲۱] (RL)

سطح ترمیم یک آسیب‌پذیری یک فاکتور مهم در الویت‌دهی است. یک آسیب‌پذیری، در زمان انتشار اولیه وصله‌ای ندارد. ابزار دور زدن آسیب‌پذیری[۲۲] یا بسته‌های ترمیم آسیب‌پذیری[۲۳] ترمیم موقتی تا زمان ارائه وصله‌های رسمی یا ترفیع‌ها هستند.

جدول ۸-امتیاز دهی به سطح ترمیم

مقدار معیار	توضیح
ترمیم آسیب‌پذیری رسمی (OF)	یک راه حل کامل که توسط تولید کنندگان، عرضه شده در دسترس است. تولید کننده یک وصله رسمی ارائه کرده یا ترفیع در دسترس است.
ترمیم آسیب‌پذیری موقتی(TF)	یک ترمیم آسیب‌پذیری رسمی ولی موقتی در دسترس است این بخش شامل مواردی می‌شود که تولید کنندگان یک بسته ترمیم آسیب پذیری یا ابزاری برای دور

[۱۸] Proof of concept

[۱۹] Functional

[۲۰] Mobile autonomous code

[۲۱] Remediation Level

[۲۲] workaround

[۲۳] hotfix

	زدن آسیب‌پذیری را ارائه می‌کنند.
دور زدن آسیب‌پذیری (W)	یک راه حل غیر رسمی که توسط تولید کننده ارائه نشده در دسترس است. در بسیاری از موارد کاربران تکنولوژیهای آسیب‌دیده، یک وصله برای خودشان تولید می‌کنند یا گامهایی برای کاهش اثر آسیب‌پذیری ارائه می‌کنند.
غیر قابل دسترس (U)	راه حلی در دسترس نیست یا به کار بردن آن غیر ممکن است.
تعریف نشده (ND)	با تخصیص این مقدار به معیار،این معیار روی امتیاز نهایی تاثیری نخواهد گذاشت.

۳-۲-۳ اطمینان از گزارش[۲۴] (RC)

این معیار میزان اطمینان از وجود آسیب‌پذیری و اعتبار جزئیات فنی را بیان می‌کند. در برخی موارد در وجود آسیب‌پذیری تردیدی نیست ولی در مورد جزئیات آن تردیدهایی وجود دارد. هرچه اطمینان از آسیب‌پذیری بیشتر باشد فوریت آن بالاتر است. مقادیر ممکن برای این معیار در جدول زیر ذکر شده‌اند هرجه آسیب‌پذیری معتبرتر باشد امتیاز بیشتری به آن تعلق خواهد گرفت.

جدول ۹-امتیاز دهی به اطمینان از گزارش

مقدار معیار	توضیح
تایید نشده[۲۵] (UN)	فقط یک منبع تایید نشده، آسیب‌پذیری را گزارش کرده است یا چندین گزارش متناقض وجود دارد که این گزارشات نیز اعتبار زیادی ندارند.
اثبات نشده[۲۶] (UR)	چندین منبع غیررسمی مانند کمپانیهای امینتی و سازمان‌های تحقیقاتی گزارشاتی داده‌اند و ممکن است بین جزئیات فنی این گزارشها تناقض وجود داشته باشد.
تایید شده (C)	آسیب‌پذیری توسط تولید کننده یا سازنده تکنولوژی تاثیر دیده تایید شده است. یک آسیب‌پذیری ممکن است از طریق وقایع خارجی مانند وجود کدهای استثمارگر عملی یا کدهایی که درستی آن‌ها اثبات شده ولی برای همه موقعیتها عملی نیست یا بهره برداریهای گسترده از آسیب‌پذیری اثبات شود.

[۲۴] Report Confidence

[۲۵] unconfirmed

[۲۶] Uncorroborated

تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار در محاسبه امتیاز نهایی تاثیری نخواهد گذاشت.

۳-۳ معیارهای محیطی

محیطهای مختلف می‌توانند بر ریسکی که توسط یک آسیب‌پذیری متوجه سازمان و کاربران آن می‌شود تاثیر گذارند. معیارهای محیطی سیستم امتیازدهی آسیب‌پذیری متعارف شامل آن دسته از ویژگیهای آسیب‌پذیری است که به محیط فناوری اطلاعات وابسته است.از آنجایی که این معیارها اختیاری هستند می‌توان با اختصاص مقادیر خاصی به این معیارها تاثیر آن‌ها بر امتیاز نهایی را از بین برد.

۳-۳-۱ خسارت بالقوه[۲۷] (CDP)

این معیار امکان از بین رفتن زندگی یا اموال فیزیکی از طریق سرقت یا خسارت به اموال و تجهیزات را اندازه‌گیری می‌کند. این معیار هم‌چنین ممکن است خسارت اقتصادی کارایی یا بازده را اندازه بگیرد. مقادیر ممکن برای این معیار در جدول ذکر شده‌اند هر چه میزان خسارت بالقوه بیشتر باشد امتیاز بیشتری به آن تعلق خواهد گرفت هر سازمانی باید یک تعریف واضح از "جزئی، متوسط، مهم، فاجعه انگیز" ارائه کند.

جدول ۱۰-امتیاز دهی به میزان خسارت بالقوه

مقدار معیار	توضیح
هیچ (N)	امکان از بین رفتن زندگی، اموال فیزیکی، بازده و کارآیی وجود ندارد.
کم (L)	یک بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی کمی دارد یا روی کارآیی یا بازدهی سازمان تاثیر کمی می گذارد.
کم-متوسط (LM)	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی متوسط دارد یا روی کارآیی یا بازدهی سازمان تاثیر متوسط دارد.
متوسط-زیاد(MH)	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی مهمی دارد یا روی کارآیی یا بازدهی سازمان تاثیر مهم دارد.
زیاد(H)	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی فاجعه‌انگیز دارد یا روی کارآیی

[۲۷] collateral damage potential

	یا بازدهی سازمان تاثیر فاجعه‌انگیز می گذارد.
تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار در محاسبه امتیاز نهایی تاثیری نخواهد گذاشت.
مقدار معیار	توضیح
هیچ (N)	امکان از بین رفتن زندگی، اموال فیزیکی، بازده و کارآیی وجود ندارد.
کم (L)	یک بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی کمی دارد یا روی کارآیی یا بازدهی سازمان تاثیر کمی می گذارد.
کم-متوسط (LM)	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی متوسط دارد یا روی کارآیی یا بازدهی سازمان تاثیر متوسط دارد.
متوسط-زیاد(MH)	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی مهمی دارد یا روی کارآیی یا بازدهی سازمان تاثیر مهم دارد.
زیاد(H)	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی فاجعه‌انگیز دارد یا روی کارآیی یا بازدهی سازمان تاثیر فاجعه‌انگیز می گذارد.
تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار در محاسبه امتیاز نهایی تاثیری نخواهد گذاشت.

۳-۳-۲ توزیع هدف[۲۸] (TD)

این معیار،درصد سیستم‌هایی که می‌توانند توسط آسیب‌پذیری تحت تاثیر قرار بگیرند را تعیین می‌کند.مقادیر ممکن برای این معیار در جدول زیر ذکر شده‌اند هرجه نسبت سیستم‌های آسیب‌پذیر بیشتر باشد امتیاز بیشتری تعلق خواهد گرفت.

جدول ۱۱-امتیاز دهی به توزیع هدف

مقدار معیار	توضیح
هیچ(N)	هیچ سیستم هدفی وجود ندارد یا اهداف بسیار تخصصی هستند و فقط در محیط آزمایشگاه وجود دارند یعنی ٪۰ از محیط در معرض ریسک قرار دارد.
کم(L)	اهداف در یک مقیاس کم در داخل محیط وجود دارند. بین ٪۲۵-٪۱ کل محیط در معرض ریسک قرار دارد.
متوسط(M)	اهداف در یک مقیاس متوسط در داخل محیط وجود دارند. بین ٪۷۵-٪۲۶ کل محیط در

[۲۸] Target Distribution

	معرض ریسک قرار دارد.
زیاد(H)	اهداف در در یک مقیاس قابل توجه در داخل محیط وجود دارند بین ٪۱۰۰-٪۷۶ کل محیط در معرض ریسک قرار دارد.
تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار روی امتیاز نهایی تاثیری نخواهد گذاشت.

۳-۳-۳نیازهای امنیتی (CR,IR,AR)

این معیار تحلیلگر را قادر می‌سازد که سیستم امتیاز دهی آسیب‌پذیری متعارف را با توجه به اهمیت منابع تاثیر دیده فناوری اطلاعات برای کاربران سازمان، تغییر دهد. اهمیت منابع با استفاده از معیارهای محرمانگی، جامعیت و در دسترس پذیری اندازه گیری می شود. به عنوان مثال اگر منابع فناوری اطلاعات از تابعی حمایت می‌کنند که در آن در دسترس پذیری عامل مهمی است تحلیلگر می‌تواند به در دسترس پذیری امتیاز بیشتری در مقایسه با جامعیت و محرمانگی اختصاص دهد. هر یک از نیازهای امنیتی سه مقدار "کم"، "متوسط" و "زیاد" می‌تواند داشته باشد.

تاثیر این معیارها بر امتیاز محیطی با استفاده از معیار پایه مربوطه تعیین می شود. یعنی این معیارها امتیاز محیطی را با دوباره وزندهی به امتیازهای پایه جامعیت، دردسترس پذیری و محرمانگی تغییر می‌دهند. به عنوان مثال وزن تاثیر محرمانگی (C) افزایش می‌یابد اگر نیاز محرمانگی (CR) "زیاد" باشد به همین صورت وزن تاثیر محرمانگی کاهش می‌یابد اگر نیاز محرمانگی "کم" باشد همین منطق برای جامعیت و در دسترس پذیری به کار می‌رود.

اگر تاثیر محرمانگی (پایه) "هیچ" قرار داده شده باشد محرمانگی روی امتیاز محیطی تاثیری نخواهد گذاشت هم‌چنین اگر معیار تاثیر (پایه) "کامل" باشد افزایش نیاز محرمانگی از "متوسط" به "زیاد" امتیاز نهایی را تغییر نخواهد داد.

جدول ۱۲-امتیاز دهی به نیازهای امنیتی

مقدار معیار	توضیح
کم (L)	از بین رفتن [محرمانگی| جامعیت|در دسترس پذیری] تاثیر محدودی روی سازمان و افرادی که باآن در ارتباط هستند (کارکنان،مشتریان) می‌گذارد.
متوسط (M)	از بین رفتن [محرمانگی| جامعیت|دردسترس پذیری] تاثیر سنگینی روی سازمان و افرادی که باآن در ارتباط هستند (کارکنان،مشتریان) می‌گذارد.
زیاد (H)	از بین رفتن [محرمانگی| جامعیت|دردسترس پذیری] تاثیر فاجعه انگیزی روی سازمان و افرادی که باآن در ارتباط هستند (کارکنان،مشتریان) می‌گذارد.
تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار روی امتیاز تاثیری نخواهد گذاشت.

۴ بردارهای پایه،موقتی و محیطی

برای نشان دادن هر معیار در بردار از نام اختصاری آن استفاده می شود.پس از نام اختصاری معیار، علامت ":" می‌آید و سپس مقادیر معیارها با نامهای اختصاری ذکر می‌شوند. بردار، این معیارها را با استفاده از یک ترتیب از پیش تعیین شده لیست می‌کند و آن‌ها را با استفاده از علامت "/" از هم جدا می‌کند. اگر از معیارهای موقتی و محیطی استفاده نشود از مقدار "ND" استفاده می‌شود. بردارهای پایه محیطی و موقتی در جدول زیر نشان داده شده‌ا ند.

جدول ۷-بردارهای پایه،موقتی و محیطی

گروه معیار	بردار
پایه	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
موقتی	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
محیطی	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/IR:[L,M,H,ND]/ AR:[L,M,H,ND]

به عنوان مثال یک آسیب‌پذیری با مقدار معیارهای پایه "بردار دسترسی: کم، پیچیدگی دسترسی: متوسط، تصدیق اصالت: هیچ، تاثیر محرمانگی : هیچ، تاثیر جامعیت: ناقص، تاثیر دردسترس پذیری :کامل" بردار پایه "AV:L/AC:M/Au:N/C:N/I:P/A:C" را خواهد داشت.

۵ امتیازدهی

این بخش نحوه امتیاز دهی سیستم امتیازدهی آسیب‌پذیری متعارف را بررسی می‌کند.در ابتدا راهنماهایی برای امتیاز دهی ارائه می‌شود سپس معادلاتی برای تولید امتیاز پایه، موقتی و محیطی تعریف می‌شوند.

۵-۱ نکات عمومی

۱. هر آسیب‌پذیری باید به طور مستقل امتیاز دهی شود.

۲. در زمان امتیازدهی به آسیب‌پذیری فقط باید تاثیر مستقیم آن روی کامپیوتر میزبان هدف در نظر گرفته شود.

۳. بسیاری از برنامه‌های کاربردی می‌توانند با مجوزهای مختلف اجرا شوند. این آسیب‌پذیریها باید با توجه به مجوزی که اغلب مورد استفاده قرار می گیرد امتیاز دهی شوند. در زمانی که اطمینان از مجوزی که اغلب مورد استفاده قرار می گیرد وجود ندارد باید از پیکربندی پیش فرض استفاده کرد.

۴. در زمان امتیاز دهی به اثر یک آسیب‌پذیری که چندین روش بهره‌برداری (استثمار) دارد تحلیلگر باید به جای انتخاب روشهایی که معمولتر هستند یا استفاده از آن‌ها آسانتر است روش استثماری را انتخاب کند که بیشترین اثر را دارد. به عنوان مثال اگر یک کد استثمارگر برای یک پلاتفورم وجود داشته باشد ولی برای پلاتفورم دیگر وجود نداشته باشد قابلت استثمار باید "در حال کار" قرار داده شود .اگر دو نسخه یک محصول به طور موازی در حال تولید باشند و یک بسته ترمیم آسیب‌پذیری برای یک نسخه وجود داشته باشد و نسخه دیگر بسته ترمیم آسیب‌پذیری نداشته باشد سطح ترمیم باید "غیر قابل دسترس" قرار داده شود.

۵-۲ معیارهای پایه

۵-۲-۱ بردار دسترسی

۵. اگر یک آسیب‌پذیری هم به صورت محلی و هم از راه شبکه قابل بهره‌برداری است مقدار "شبکه" باید انتخاب شود وقتی یک آسیب‌پذیری هم به صورت محلی قابل بهره‌برداری است و هم از طریق شبکه مجاور ولی از طریق شبکه راه دور قابل بهره‌برداری نیست مقدار "شبکه مجاور" باید انتخاب شود اگر یک آسیب‌پذیری از طریق شبکه مجاور و هم از طریق شبکه راه دور قابل بهره‌برداری باشد، مقدار "شبکه" باید انتخاب شود.

۶. بسیاری از برنامه‌های کاربردی سرویس گیرنده آسیب‌پذیریهای محلی دارند که می‌توانند از راه دور از طریق کاربران یا فرآیندهای اتوماتیک مورد بهره‌برداری قرار گیرند به عنوان مثال برنامه‌های پویش ویروس به طور اتوماتیک همه پستهای الکترونیک ورودی را پویش می‌کنند. *"برنامه‌های کاربردی کمک کننده"*[۲۹] (ناظرین تصویر[۳۰]،پخش کننده فایلهای رسانه‌ای[۳۱])زمانی که فایل‌های مخرب از طریق پست الکترونیک مبادله شوند یا از

---

[۲۹] Helper application

[۳۰] Image viewers

[۳۱] Media player

وب سایت‌ها دانلود شوند مورد بهره‌برداری قرار می گیرند بنابراین تحلیلگر باید بردار دسترسی این آسیب‌پذیریها را "شبکه" قرار دهد.

۵-۲-۲ تصدیق اصالت

۷. اگر در رویه تصدیق اصالت آسیب‌پذیری وجود داشته باشد (Kerberos) یا برای سرویس‌های ناشناس[۳۲] (سرور FTP عمومی) این معیار باید با "هیچ" امتیاز دهی شود زیرا حمله‌کننده می‌تواند بدون فراهم کردن شناسه کاربری و کلمه عبور معتبر از آسیب‌پذیری بهره‌برداری کند در صورت وجود یک حساب کاربری پیش فرض مقدار این معیار را می‌توان "واحد" یا "متعدد"در نظر گرفت. اگر شناسه کاربری و کلمه عبور در دسترس عموم باشد قابلیت بهره‌برداری باید مقدار "زیاد" را بگیرد.

۵-۲-۳ تاثیرهای محرمانگی،جامعیت و در دسترس پذیری

۸. آسیب‌پذیریهایی که دسترسی در سطح ریشه را فراهم می‌کنند باید با تخریب کامل محرمانگی، در دسترس پذیری و جامعیت امتیاز دهی شوند و آسیب‌پذیریهایی که دسترسی در سطح کاربر را فراهم می‌کنند با تخریب بخشی از محرمانگی، در دسترس پذیری و جامعیت امتیاز دهی می‌شوند. یک نقض جامعیت که به حمله‌کننده اجازه می‌دهد که فایل کلمه عبور سیستم عامل را تغییر دهد باید با تاثیر کامل محرمانگی، در دسترس پذیری و جامعیت امتیاز دهی شود.

۹. آسیب‌پذیریها با تخریب ناقص یا کامل جامعیت می‌توانند بر در دسترس پذیری نیز اثر گذارند به عنوان مثال یک حمله‌کننده که می‌تواند رکوردها را تغییر دهد می‌تواند آن‌ها را حذف نیز کند.

۵-۲-۴معادله پایه

معادله پایه، اساس امتیاز دهی سیستم امتیازدهی آسیب‌پذیری متعارف است. معادله پایه به این صورت است:

```
BaseScore = round_to_۱_decimal(((۰٫۶*Impact)+(۰٫۴*Exploitability)-
۱٫۵)*f(Impact))
```

[۳۲] anonymous

```
Impact = ۱۰٫۴۱*(۱-(۱-ConfImpact)*(۱-IntegImpact)*(۱-AvailImpact))

Exploitability = ۲۰* AccessVector*AccessComplexity*Authentication

f(impact)= ۰ if Impact=۰, ۱٫۱۷۶ otherwise


AccessVector = case AccessVector of
        requires local access: ۰٫۳۹۵
        adjacent network accessible: ۰٫۶۴۶
        network accessible: ۱٫۰


AccessComplexity = case AccessComplexity of
         high: ۰٫۳۵
         medium: ۰٫۶۱
         low: ۰٫۷۱


Authentication = case Authentication of
         requires multiple instances of authentication: ۰٫۴۵
         requires single instance of authentication: ۰٫۵۶
         requires no authentication: ۰٫۷۰۴


ConfImpact = case ConfidentialityImpact of
                none: ۰٫۰
       partial: ۰٫۲۷۵
       complete: ۰٫۶۶۰


IntegImpact = case IntegrityImpact of
        none: ۰٫۰
        partial: ۰٫۲۷۵
        complete: ۰٫۶۶۰
```

```
AvailImpact = case AvailabilityImpact of
        none: ۰٫۰
        partial: ۰٫۲۷۵
                complete: ۰٫۶۶۰
```

۵-۲-۵معادله موقتی

اگر از این معادله استفاده شود معیارهای موقتی با امتیاز پایه ترکیب می‌شوند تا امتیاز موقتی که از ۰ تا ۱۰ تغییر می‌کند تولید شود به علاوه توسط این معادله امتیازی تولید می‌شود که از امتیاز پایه بیشتر نخواهد بود و از ٪۳۳ امتیاز پایه نیز کمتر نخواهد شد.معادله موقتی به این صورت است:

```
TemporalScore = round_to_۱_decimal(BaseScore*Exploitability
       *RemediationLevel*ReportConfidence)

Exploitability = case Exploitability of
         unproven: ۰٫۸۵
         proof-of-concept: ۰٫۹
         functional: ۰٫۹۵
         high: ۱٫۰۰
         not defined: ۱٫۰۰

RemediationLevel = case RemediationLevel of
          official-fix: ۰٫۸۷
          temporary-fix: ۰٫۹۰
          workaround: ۰٫۹۵
          unavailable: ۱٫۰۰
```

```
            not defined: ۱،۰۰


   ReportConfidence = case ReportConfidence of
            unconfirmed: ۰،۹۰
            uncorroborated: ۰،۹۵
            confirmed: ۱،۰۰
            not defined: ۱،۰۰
```

۵-۲-۶معادله محیطی

در صورت استفاده از این معادله معیارهای محیطی با امتیاز موقت ترکیب شده و امتیاز محیطی که از ۰ تا ۱۰ تغییر می‌کند تولید خواهد شد. این معادله، امتیازی تولید می‌کند که از امتیاز موقتی بیشتر نخواهد بود. معادله محیطی به این صورت است:

```
   EnvironmentalScore = round_to_۱_decimal((AdjustedTemporal+
   (۱۰-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)


   AdjustedTemporal = TemporalScore recomputed with the BaseScore's Impact
subequation
   replaced with the AdjustedImpact equation


   AdjustedImpact         =         min(۱۰،۱۰،۴۱*(۱-(۱-ConfImpact*ConfReq)*(۱-
IntegImpact*IntegReq)
         *(۱-AvailImpact*AvailReq)))


   CollateralDamagePotential = case CollateralDamagePotential of
               none: ۰
               low: ۰،۱
```

```
                low-medium: ۰٫۳
                medium-high: ۰٫۴
                high: ۰٫۵
                not defined: ۰

TargetDistribution = case TargetDistribution of
            none: ۰
            low: ۰٫۲۵
            medium: ۰٫۷۵
            high: ۱٫۰۰
            not defined: ۱٫۰۰

ConfReq = case ConfReq of
       low: ۰٫۵
       medium: ۱٫۰
       high: ۱٫۵۱
       not defined: ۱٫۰

IntegReq = case IntegReq of
        low: ۰٫۵
        medium: ۱٫۰
        high: ۱٫۵۱
        not defined: ۱٫۰

AvailReq = case AvailReq of
        low: ۰٫۵
        medium: ۱٫۰
        high: ۱٫۵۱
```

```
not defined: ۱.۰
```

۶ منابع و مراجع

۱. Mell, P.,Scarfon ,K.,Romanosky ,S., *A Complete Guide to the Common Vulnerability Scoring System Version* ۲.۰ Available at http://www.first.org/cvss/cvss-guide.html .