ارائه مدلی برای بهبود روند امتیازدهی به آسیب‌پذیری در CVSS

مرجان کرامتی[1]

۱- مربی- دانشکده ریاضی، آمار و علوم کامپیوتر-دانشگاه سمنان- سمنان-ایران

Keramati_marjan@semnan.ac.ir

چکیده: امروزه حملات سایبری را می‌توان یکی از نگرانی‌های اصلی زندگی بشر به حساب آورد. بنابراین به‌منظور مقاوم‌سازی شبکه در مقابل حملات سایبری به عنوان یک دغدغه اساسی متخصیصن امنیتی، نیازمند اولویت‌بندی آسیب‌پذیری‌ها و انتخاب پرخطرترین آنها هستیم. در نتیجه، ارزیابی دقیق خطر آسیب‌پذیری‌ها اهمیت بالایی دارد. سیستم امتیازدهی به آسیب‌پذیری CVSS به عنوان یکی از محبوب‌ترین سیستم‌های امتیازدهی به آسیب‌پذیری دارای یکسری مشکلات اساسی است که ارزیابی خطر دقیق حملات را دچار مشکل می‌سازد. دامنه محدود امتیازها در CVSS را می‌توان یکی از مشکلات اساسی این سیستم امتیازدهی به آسیب‌پذیری به حساب آورد. چرا که مجزاسازی کارای سیل عظیمی از آسیب‌پذیری‌ها توسط این سیستم را غیر ممکن می‌سازد. در این مقاله روشی برای اصلاح روند امتیازدهی به آسیب‌پذیری با محوریت چالش مذکور و افزایش دقت تخمین خطر حملات معرفی شده است.

واژه‌های کلیدی: دسترسی پذیری، محرمانگی، CVSS ، Exploitability، Impact، صحت داده، مقاوم‌سازی شبکه، خطر، آسیب پذیری

نوع مقاله: پژوهشی

DOI: 10.52547/jiaeee.19.1.35

تاریخ ارسال مقاله : ۱۳۹۷/۰۴/۱۳

تاریخ پذیرش مشروط مقاله: ۱۳۹۷/۱۰/۲۲

تاریخ پذیرش مقاله: ۱۳۹۸/۰۹/۲۱

نام نویسنده‌ی مسئول: مرجان کرامتی

نشانی نویسنده‌ی مسئول: ایران – سمنان – کیلومتر ۵ جاده دامغان– دانشگاه سمنان – دانشکده ریاضی آمارو علوم کامپیوتر

۱- مقدمه

در عصر تکنولوژی وابستگی جنبه‌های مختلف زندگی بشر به شبکه های کامپیوتری امری اجتناب‌ناپذیر است. بنابراین، مقاوم‌سازی سیستم‌های کامپیوتری در برابر رفتارهای تبهکارانه یک ضرورت اساسی به حساب خواهد آمد و این امر ممکن نخواهد بود جز با ارزیابی خطر حملات و ممانعت از وقوع پرخطرترین حملات.

حذف پیش‌شرط‌های مورد نیاز برای وقوع حمله و اعمال اصلاحیه برای آسیب‌پذیری‌ها، دو روش مرسوم برای ممانعت از وقوع حملات به شمار می‌آیند. توجه به این نکته حائز اهمیت است که، حذف پیش-شرط‌های مورد نیاز برای وقوع حمله را می‌توان معادل دانست با محدود کردن قوانین فایروال که به تبع آن دسترسی کابران مجاز به سیستم نیز محدود خواهد شد. تفسیری از تبعات مقاوم‌سازی شبکه در برابر حملات برای کاربران را می‌توان هزینه مقاوم‌سازی تعبیر کرد که هم می‌تواند ماهیت مادی داشته باشد و هم ماهیت غیر مادی.

در فرآیند مقاوم‌سازی، هزینه همواره یک عامل محدود کننده خواهد بود. در نتیجه باید دقت داشت که مقاوم‌سازی به صورت کم-هزینه انجام شود. به عبارت دیگر در فرآیند مقاوم‌سازی شبکه نیازمند این خواهیم بود که پرخطرترین حملات مشخص و هزینه صرفا برای برطرف‌سازی این حملات صرف شود. بنابراین، در فرآیند مقاوم‌سازی شبکه، ارزیابی خطر حملات اهمیت ویژه‌ای پیدا می‌کند.

ارزیابی احتمال وقوع حمله و تبعات ناشی از وقوع حمله در قالب آسیب به پارامترهای امنیتی دسترسی‌پذیری، محرمانگی و صحت‌داده دو فاکتور اساسی در ارزیابی خطر یک حمله هستند. به عبارت دیگر، ارزیابی خطر یک حمله طبق رابطه (۱) محاسبه می‌شود [۱]:

پارامترهای موجود در این رابطه عبارتند از:

- Likelihood of an adverse event : احتمال رخداد حمله
- Impact of the adverse event: تاثیر مخرب رخداد حمله روی سه پارامتر امنیتی محرمانگی، صحت داده و دسترسی‌پذیری است.

$$Risk = Likelihood\ of\ an\ adverse\ event \times Impact\ of\ the\ adverse\ event. \quad (1)$$

سیستم‌های متعددی وجود دارند که ارزیابی خطر را برای صرفا یک آسیب‌پذیری انجام می‌دهند. CVSS و CWE دو نمونه از این سیستم‌ها هستند [۲] و [۳]. اما یکسری مشکلات اساسی وجود دارد که استفاده کارا از این سیستم‌ها را در عمل غیر ممکن می‌سازد. یک مشکل اساسی وجود صرفا تعدادی معدودی امتیاز برای امتیازدهی به سیل عظیمی از آسیب‌پذیری‌ها است که مجزاسازی کارای حملات از نقطه نظر خطر وارده به سیستم را دچار مشکل می‌سازد.

در کارهای پیشین [۷-۴]، ما روشی برای ارزیابی خطر حملات چند مرحله‌ای ارائه داده‌ایم. حملات چند مرحله‌ای حملاتی هستند که در آن مهاجم چندین آسیب‌پذیری با یک ترتیب مشخص را جهت رسیدن به نقطه هدف مورد بهره‌برداری قرار می‌دهد.

در این مقاله هدف بهبود سیستم امتیازدهی به آسیب‌پذیری CVSS از نقطه نظر افزایش دقت و افزایش گستره امتیازت در این سیستم ارزیابی خطر است. تمرکز روش پیشنهادی در افزایش دقت ارزیابی تاثیر بهره‌برداری از آسیب‌پذیری روی سه پارامتر محرمانگی، صحت داده و دسترسی‌پذیری است.

در [۶] ما روشی برای بهبود گستره امتیازات در نسخه ۲ از CVSS انجام دادیم. در این مقاله تمرکز برای روی اصلاح گستره امتیازات در نسخه ۳ از CVSS است.

در ادامه پس از مرور کوتاهی بر تعدادی از کارهای مشابه در بخش ۲، چالش‌های سیستم CVSS در بخش ۳ معرفی می‌شوند . سپس بعد از معرفی روش پیشنهادی در بخش ۴، کارایی روش پیشنهای با مقایسه نتایج با CVSS، مورد بررسی قرار می‌گیرد.

۲- کارهای مشابه

در ادامه تعدادی از سیستم‌های استاندارد و غیر استانداردی موجود برای ارزیابی خطر آسیب‌پذیری‌ها مورد بررسی قرار می‌گیرد.

۲-۱- سیستم‌های استاندارد

- سیستم Microsoft Security Response Center

سیستم با برآورد احتمال بهره‌برداری از هر یک از آسیب پذیری های ثبت شده، اولویت توسعه اصلاحیه برای هر آسیب‌پذیری را مشخص می‌سازد [۸].

- سیستم Symantec

در این سیستم، پنج سطح کیفی برای ارزیابی خطر آسیب پذیری‌ها وجود دارد. در این سیستم همچنین راهکارهایی برای کاهش اثرات مخرب ناشی از بهره برداری از هر آسیب‌پذیری پیشنهاد می‌شود [۹].

- سیستم CVSS

این سیستم به عنوان یک سیستم محبوب ارزیابی خطر آسیب پذیری، سطح خطر هر تک آسیب‌پذیری را به صورت کمی و کیفی مشخص می‌سازد[۲]. در بخش‌های آتی جزئیات بیشتری از این سیستم ارزیابی خطر بیان خواهد شد.

- سیستم RedHat

این سیستم، ارزیابی خطر آسیب‌پذیری‌های محصولات RedHat را در چهار سطح کیفی مشخص می‌سازد[۱۰]. در این سیستم با اولویت‌بندی آسیب‌پذیری‌ها، زمانبندی توسعه اصلاحیه مشخص می شود[۱۰].

۲-۲- سیستم‌های غیر استاندارد

در سال‌های اخیر تلاش‌های قابل توجهی در رابطه با ارزیابی خطر آسیب‌پذیری‌ها و بهبود سیستم‌های ارزیابی خطر موجود انجام شده است. در ادامه مروری داریم بر تعدادی از تلاش‌های فوق.

در [۱۱]، با هدف بهبود گستره آسیب‌پذیری‌ها و اصلاح توزیع امتیازات در CVSS، تعدادی معیار امنیتی معرفی شده است.

در [۱۲]، روشی برای ارزیابی شدت خطر هر میزبان ارائه شده است. نوآوری روش پیشنهادی را می‌توان بهبود دقت خطر برآورده شده از حملات نسبت به CVSS دانست. چرا که در سیستم پیشنهادی، معیارهای زمانی (احتمال توسعه اصلاحیه و احتمال توسعه اکسپلویت) نیز در کنار معیارهای پایه CVSS، برای ارزیابی خطر مورد استفاده قرار می‌گیرد.

در [۱۳] بهبود ارزیابی خطر آسیب‌پذیری نسبت به CVSS با اصلاح فرمول‌ها و دخیل کردن عوامل محیطی انجام می‌شود. در [۱۴] نیز روشی برای بهبود پراکندگی امتیازت در CVSS پیشنهاد شده است.

در [۶]، ما چارچوبی برای ارزیابی خطر آسیب‌پذیری پیشنهاد دادیم روش پیشنهادی بهبودی است بر سیستم امتیازدهی CVSS. در سیستم پیشنهادی تلاش شده است که، گستره امتیازات سیستم مذکور با در نظر گرفتن عوامل زمانی و اصلاح روش ارزیابی تاثیر بهره برداری از آسیب‌پذیری روی پارامترهای امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری بهبود پیدا بکند.

همان‌طور که قبلا نیز اشاره شد، نقطه ضعف اساسی CVSS، گستره پایین امتیازات و به تبع آن دقت پایین ارزیابی خطر انجام شده است.

در این مقاله، روشی برای بهبود تاثیر بهره‌برداری از آسیب‌پذیری روی پارامترهای محرمانگی، یکپارچگی و دسترسی پذیری در نسخه ۳ از CVSS پیشنهاد شده است که کارایی ارزیابی خطر را با افزایش گستره امتیازات و دقت، بالا می‌برد.

۳- مروری بر سیستم امتیازدهی CVSS و چالش‌های آن

در این بخش بعد از مرور کوتاهی بر CVSS، تعدادی از چالش های آن مورد بحث قرار می‌گیرند.

۳-۱- مرور مختصری بر CVSS

سیستم امتیازدهی CVSS یکی از محبوب‌ترین سیستم‌های ارزیابی خطر آسیب‌پذیری است که وجود محاسبه‌گر امتیاز، را می‌توان یک ویژگی کلیدی برای این سیستم امتیازدهی به حساب آورد.

جدیدترین نسخه محاسبه گر موجود برای CVSS نسخه ۳ است که امتیازدهی به آسیب‌پذیری‌ها را برای موارد ثبت شده از سال ۲۰۱۶ و تعدادی از موارد ثبت شده قبل از ۲۰۱۶ انجام می‌دهد. سه گروه اصلی از معیارها برای ارزیابی خطر در این سیستم امتیازدهی پیشنهاد شده است که در حال حاضر، محاسبه خطر در سیستم پیشنهادی براساس Base Score انجام می‌شود [۲]:

- گروهBase Score : این گروه از معیارها نمایانگر خصوصیات اساسی و ذاتی آسیب‌پذیری‌هاست که با گذر زمان و به واسطه قرار گرفتن در محیطهه و شبکه‌های مختلف تغییری در آن حاصل نمی‌شود.
- گروه Temporal Score : بیانگر خصوصیاتی از آسیب پذیری است که در گذر زمان تغییر می‌کند (احتمال توسعه اصلاحیه و احتمال توسعه اکسپلویت) ولی بهره‌برداری از آسیب‌پذیری در محیط‌های گوناگون تغییری در امتیاز گزارش شده ایجاد نمی‌کند.
- گروه Environmental Score : این گروه از امتیازات بیانگر مشخصه‌هایی از آسیب‌پذیری هستند که به واسطه قرار گرفتن در شبکه‌های مختلف متفاوت خواهد بود.

محاسبه‌گر CVSS، با دریافت شناسه CVE هر آسیب‌پذیری ثبت شده، خطر آسیب‌پذیری را بر اساس پارامترهای گروه پایه آسیب پذیری گزارش می‌کند. CVE را می‌توان یک دیکشنری از تمامی آسیب‌پذیری‌های ایندکس شده به حساب آورد [۱۵].

همان‌طور که اشاره شد، CVSS خطر متناظر با بهره‌برداری از هر آسیب‌پذیری را صرفا براساس پارامترهای پایه انجام می‌دهد. بنابراین، روش پیشنهادی در این مقاله نیز بهبود امتیازدهی را بر اساس پارامترهای گروه پایه این سیستم امتیازدهی انجام می‌دهد. معیارهای پایه‌ای CVSS در دودسته کلی زیر قرار می گیرند.

- Exploitability : درجه سختی بهره‌برداری از هر آسیب‌پذیری را مشخص می‌سازد.
- Impact : تاثیر بهره‌برداری از هر آسیب‌پذیری را بر روی سه پارامتر امنیتی محرمانگی، صحت داده و دسترسی‌پذیری مشخص می‌سازد.

در این مقاله، تمرکز بر روی بهبود پارامتر Impact از CVSS است.

۳-۲- مروری بر تعدادی از چالش‌های CVSS

تعدادی از چالش‌های اساسی سیستم CVSS عبارتند از :

- از آنجایی که پارامترهای زمانی در ارزیابی خطر انجام شده توسط CVSS نادیده گرفته می‌شود. میزان خطر گزارش شده، اثر معرفی اصلاحیه برای آسیب پذیری‌ها و ابزارهای بهره‌برداری از آسیب‌پذیری در گذر زمان را نادیده می‌گیرد.
- مشکل اساسی دیگر CVSS که می‌توان به آن اشاره داشت این است که تنها محدوده کوچکی از اعداد

برای امتیازدهی به سیل عظیمی از آسیب‌پذیری‌ها موجود است. بنابراین، اولویت‌بندی انجام شده توسط این سیستم امیتیازدهی برای تعیین پر خطر ترین حمله مناسب نخواهد بود.

- نکته قابل توجه دیگر این است که CVSS، اهمیت نسبی پارامترهای امنیتی دسترسی‌پذیری، محرمانگی و صحت اطلاعات را نادیده می‌گیرد. این در صورتی است که از آنجا که درجه سختی تشخیص نقض شدن محرمانگی از صحت اطلاعات و درجه سختی نقض شدن صحت اطلاعات از دسترسی‌پذیری بیشتر است، نادیده گرفتن این اهمیت نسبی، دقت میزان خطر گزارش شده را تحت تاثیر قرار می‌دهد.
- ماهیت متفارن فرمول Impact در این سیستم امتیازدهی ویژگی دیگری است که گستردگی امتیازات در این سیستم امتیازدهی را کاهش داده است.

در این مقاله با هدف بهبود گستره امتیازات و افزایش دقت ارزیابی خطر انجام شده در CVSS، مدل‌هایی برای بهبود دو چالش اخیر معرفی شده است.

۴- روش پیشنهادی

طبق فرمول (۱)، ارزیابی پارامتر Impact یکی از اجزای اساسی فرآیند ارزیابی خطر آسیب‌پذیری است. نوآوری مقاله پیشنهادی را می‌توان اصلاح پارامتر Impact با لحاظ کردن دو مورد زیر در نظر گرفت:

- تغییر ساختار متقارن محاسبه‌گر Impact در سیستم CVSS
- در نظر گرفتن اهمیت نسبی سه پارامتر امنیتی محرمانگی، صحت اطلاعات و دسترسی پذیری

در [۶]، ما روشی برای بهبود پارامتر Impact با تمرکز بر دو مورد مذکور برای نسخه ۲ از CVSS ارائه دادیم .در مقاله پیش رو ، روش معرفی شده در [۶] برای نسخه ۳ از سیستم CVSS توسعه داده شده است..

برای هر آسیب‌پذیری ایندکس شده با شناسه CVE، محاسبه‌گر CVSS، یکی از مقادیر را به عنوان تاثیر مخرب بهره‌برداری از آسیب پذیری روی سه پارامتر محرمانگی، یکپارچگی و دسترسی‌پذیری گزارش می‌کند.

- None (0)
- Low (0.22)
- High (0.56)

همان‌طور که در بخش قبل ذکر شد، یک مشکل اساسی CVSS این است که محاسبه‌گر Impact برای سطوح یکسان هر یک از سه پارامتر امنیتی مذکور سطح کمی مشابهی را گزارش می‌کند. این ویژگی به همراه ماهیت متقارن محاسبه‌گر Impact، دقت خطر گزارش شده و گستره امتیازات خطر در CVSS را کاهش می‌دهد.

در CVSS به دلیل ماهیت متقارن محاسبه‌گر Impact، برای آسیب‌پذیری‌های که در از نقطه نظر تاثیر مخرب روی پارامترهای امنیتی در دسته‌های مشابه قرار دارند، عدد یکسانی برای Impact گزارش می‌شود. (هر یک از ترکیب‌های سه تایی، از چپ به راست، تاثیر مخرب آسیب‌پذیری را روی پارامترهای محرمانگی، یکپارچگی و دسترسی‌پذیری مشخص می‌سازد.)

- {nhn, hnn, nnh}
- {nln, lnn, nnl}
- {nln, lnn, nnl}
- {nhh, hhn, hnh}
- {nll, lln ,lnl}
- {nhl,lhn,hln,hnl,nlh,hnl}

روابط (۲) و (۳) محاسبه‌گر Impact در CVSS را مشخص می سازد. در این دو فرمول، $Impact_{Conf}$ ، $Impact_{Integ}$ ، $Impact_{Avail}$ به ترتیب، تاثیر مخرب بهره‌برداری از آسیب‌پذیری را روی سه پارامتر امنیتی محرمانگی، صحت اطلاعات و دسترسی‌پذیری گزارش می‌کند.

$$Impact = \begin{cases} 6.42 \times ISC_{Base}, & Scope \quad Unchanged \\ 7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15} & Scope \quad Changed \end{cases} \quad (۲)$$

$$ISC_{Base} = 1 - \left[\begin{matrix} (1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times \\ (1 - Impact_{Avail}) \end{matrix} \right] \quad (۳)$$

یکی از نوآوری‌های مقاله پیش‌رو، تلاش برای شکستن ساختار متقارن محاسبه‌گر Impact است که این کار با وزن‌دار کردن سه پارامتر امنیتی مذکور و با در نظر گرفتن اهمیت نسبی آنها انجام شده است. همچنین تلاش شده است که برای سطوح کیفی یکسان تخریب برای هر پارامتر امنیتی، عدد متفاوتی براساس درجه اهمیت آن پارامتر نسبت داده شود.

در روش پیشنهادی تلاش شده است که با نرمال‌سازی‌هایی که انجام می‌شود، محدود اعداد گزارش شده توسط محاسبه‌گرImpact با CVSS یکسان باشد. بنابراین، مقادیر کمی متناظر با ترکیب lll و hhh همان مقادیر گزارش شده در CVSS خواهد بود. در واقع دو فرض اساسی برای حل مسئله مذکور در این مقاله به شرح زیر خوئاهد بود:

۱. اهمیت نسبی سه پارامتر امنیتی مذکور
۲. مقادیر متناظر با Impact برای ترکیب‌های lll و hhh

روابط (۴) الی (۶) براساس دو فرض مذکور استخراج شده و به شرح زیر هستند:

$$\left[(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail}) \right] \quad (۴)$$

$$\begin{bmatrix}(1-Impact_{Conf})\times(1-Impact_{Integ})\times\\(1-Impact_{Avail})\end{bmatrix}=0.085184 \quad (۵)$$

$$Impact_{Conf}=Impact_{Integ}=Impact_{Avail}=high$$

$$Impact_{Conf}>Impact_{Integ}>Impact_{Avail}$$

$$2^{*}\times Impact_{Avail}>Impact_{Integ}$$
$$2\times Impact_{Integ}>Impact_{Conf}$$
$$Impact_{Avail}>Impact_{Conf}\times 1/3$$

$$Impact_{Integ}>Impact_{Conf}\times 2/3$$

$$\begin{bmatrix}(1-Impact_{Conf})\times(1-Impact_{Integ})\\\times(1-Impact_{Avail})\end{bmatrix}=0.474552 \quad (۶)$$

$$Impact_{Conf}=Impact_{Integ}=Impact_{Avail}=low$$
$$Impact_{Conf}>Impact_{Integ}>Impact_{Avail}$$
$$2^{*}\times Impact_{Avail}>Impact_{Integ}$$
$$2\times Impact_{Integ}>Impact_{Conf}$$
$$Impact_{Avail}>Impact_{Conf}\times 1/3$$
$$Impact_{Integ}>Impact_{Conf}\times 2/3$$

با حل معادلات روابط (۵) و (۶)، ضرایب موجود در جدول ۱ به عنوان مقادیر ممکن برای سطوح بالا و پایین سطوح امنیتی سه پارامتر امنیتی مذکور استخراج می‌شود.

در جدول (۱)، {CH, IH, AH} و {CL, IL, AL} عبارتند از مقادیر عددی متناظر با سطوح بالا و پایین پارامترهای $Impact_{Conf}$, $Impact_{Integ}$ and $Impact_{Avail}$.

همان طور که در جدول (۱) مشاهده می‌شود برای مقادیر سطوح پایین تنها {CH, IH, AH}= {0.28,0.22,0.1550} گزارش شده است ولی برای مقادیر سطح بالا انتخاب‌های متعددی وجود دارد. (روابط (۷) و (۸))

بنابراین، باید تلاش شود از بین مقادیر گزارش شده تنها یک مقدار برای {CH, IH, AH} استخراج گردد.

همان‌طور که قبلا نیز اشاره شد، CVSS به ترتیب، ۰/۲۲ و ۰/۵۶ را برای مقادیر بالا و پایین تخصیص می‌دهد. بنابراین، با هدف سازگار ساختن هر چه بیشتر روش پیشنهادی با سیاست‌های CVSS و استخراج مقدار عددی متناظر با {CH, IH, AH}، رابطه (۹) تعریف شده است. همچنین رابطه (۱۰) نیز فاصله بین بردار (۹) با هریک از بردارهای موجود در (۷) را مشخص می‌سازد.

جدول (۱): مقادیر عددی حاصل از حل معادلات (۵) و (۶)

CH	CL	AH	AL	IH	IL
۰/۶۴۸	۰/۲۸	۰/۵	۰/۱۵۵۰	۰/۵۱۶۰	۰/۲۲
۰/۶۴۸		۰/۳۹۵		۰/۶	
۰/۶۸		۰/۴۵		۰/۵۱۶۰	
۰/۷۲۵		۰/۳۹۵		۰/۴۴۸	
۰/۷۵		۰/۲۹۶		۰/۵۱۶	

$$\begin{matrix}CH & AH & IH\end{matrix}$$

$$\begin{pmatrix}0.648 & 0.5 & 0.5160\\0.648 & 0.395 & 0.6\\0.68 & 0.45 & 0.516\\0.725 & 0.395 & 0.488\\0.75 & 0.296 & 0.516\end{pmatrix} \quad (۷)$$

$$Low=\{\text{CL, IL, AL}\}=\begin{pmatrix}0.28 & 0.22 & 0.1550\end{pmatrix} \quad (۸)$$

$$Index=\frac{0.56}{0.22}\times Low \quad (۹)$$

$$distance=\begin{bmatrix}0.1313\\0.0761\\0.078\\0.0730\\0.1142\end{bmatrix} \quad (۱۰)$$

هدف از محاسبه بردار فاصله در (۹)، پیدا کردن برداری عددی برای {CH, IH, AH} است که از نقطه نظر حفظ نسبت (۰/۵۶ به ۰/۲۲) بین مقادیر بالا و پایین Impact بهینه باشد. بنابراین، بردار عددی متناظر با کوچکترین مقدار موجود در ماتریس (۱۰) به عنوان مقدار عددی متناظر با .{CH, IH, AH} انتخاب می‌شود.

همان طور که اشاره شد، یکی از نوآوری‌های مقاله پیش رو، اصلاح روند امتیازدهی به Impact بر اساس اهمیت نسبی سه پارامتر امنیتی محرمانگی، صحت اطلاعات و دسترسی‌پذیری است. مقادیر عددی تخصیص داده شده به زیر پارامترهای Impact در CVSS و سیستم پیشنهادی در جدول (۲) نشان داده شده است.

با تجزیه و تحلیل جدول (۲)، اهمیت نسبی سه پارامتر امینتی در روش پیشنهادی مشهود است. بنابراین، در روش پیشنهادی بر خلاف CVSS، برای هر یک از اعضای هر کدام از مجموعه‌های زیر، مقادیر متفاوتی برای تاثیر بهره‌برداری از آسیب‌پذیری روی پارامترهای امنیتی گزارش می‌شود.

- {nhn, hnn, nnh}
- {nln, lnn, nnl}
- {nln, lnn, nnl}
- {nhh, hhn, hnh}
- {nll, lln ,lnl}
- {nhl,lhn,hln,hnl,nlh,hnl}

جدول (۲): مقادیر عددی زیر پارامتر Impact در CVSS و سیستم پیشنهادی

	CH	IH	AH	CL	IL	AL
CVSS	۰/۵۶	۰/۵۶	۰/۵۶	۰/۲۲	۰/۲۲	۰/۲۲
روش پیشنهادی	۰/۷۲۵	۰/۴۴۸	۰/۳۹۵	۰/۲۸	۰/۲۲	۰/۱۵۵۰

۵- مقایسه کارایی روش پیشنهادی و CVSS

در جدول (۳)، مقادیر عددی رابطه (۴) برای هر یک از ترکیب های ممکن از سه پارامتر امنیتی برای سیستم پیشنهادی وCVSS نشان داده شده است. (هر ترکیب ۳ تایی از چپ به راست درجه آسیب بهره‌برداری از آسیب‌پذیری را روی سه پارامتر امنیتی محرمانگی، صحت اطلاعات و دسترسی‌پذیری مشخص می‌سازد)

طبق اطلاعات موجود در جدول (۳)، مشخص است که پراکندگی امتیازات در روش پیشنهادی نسبت به CVSS بهبود پیدا کرده است. از طرفی، در نظر گرفتن اهمیت نسبی سه پارامتر امنیتی، دقت ارزیابی خطر را نیز نسبت به CVSS بهبود داده است.

جدول (۳): مقادیر عددی متناظر با زیر پارامترهای ممکن در Impact در CVSS و سیستم پیشنهادی

زیرپارامتر های Impact	CVSS	روش پیشنهادی	زیرپارامتر های Impact	CVSS	روش پیشنهادی	زیرپارامتر های Impact	CVSS	روش پیشنهادی
nnn	۱	۱	nll	۰/۶۹۸۴	۰/۶۹۵۱	hln	۰/۳۴۳۲	۰/۲۱۴۵
lll	۰/۴۲۷۶	۰/۴۲۷۶	lln	۰/۶۰۸۴	۰/۵۱۸۴	lhn	۰/۳۴۳۲	۰/۳۶۸۶
hhh	۰/۸۵۲	۰/۸۵۲	lnl	۰/۶۰۸۴	۰/۶۰۸۴	lnh	۰/۳۴۳۲	۰/۴۳۵۶
nnl	۰/۷۸	۰/۸۴۵	nhh	۰/۱۹۳۶	۰/۳۰۹۸	lhh	۰/۱۵۱۰	۰/۲۲۳۰
nln	۰/۷۸	۰/۷۸	hhn	۰/۱۹۳۶	۰/۱۴۰۸	hlh	۰/۱۵۱۰	۰/۱۲۹۸
lnn	۰/۷۸	۰/۷۲	hnh	۰/۱۹۳۶	۰/۱۶۶۴	hhl	۰/۱۵۱۰	۰/۱۱۹۰
nnh	۰/۴۴	۰/۶۰۵	nhl	۰/۳۴۳۲	۰/۴۳۲۶	llh	۰/۲۶۷۷	۰/۳۳۹۸
nhn	۰/۴۴	۰/۵۱۲	hnl	۰/۳۴۳۲	۰/۲۳۲۴	hll	۰/۲۶۷۷	۰/۱۸۳۰
hnn	۰/۴۴	۰/۲۷۵	nlh	۰/۳۴۳۲	۰/۴۷۱۹	lhl	۰/۲۶۷۷	۰/۳۱۱۵

۶- نتیجه‌گیری

نظر به گستره وسیع حملات سایبری، مقاوم‌سازی کم‌هزینه را می‌توان به عنوان یک ضرورت اجتناب‌ناپذیر در شبکه‌های کامپیوتری تصور کرد. این امر ممکن نخواهد بود جز با، ارزیابی خطر حملات و اولویت‌بندی به منظور تعیین پرخطرترین آنها. در نتیجه، ارزیابی خطر به عنوان یک فاکتور کلیدی در محافظت از شبکه‌های کامپیوتری در نظر گرفته می‌شود. CVSS به عنوان محبوب‌ترین و پرکاربردترین سیستم امتیازدهی به آسیب‌پذیری یکسری نقطه ضعف اساسی دارد. گستره پایین امتیازات در CVSS را می‌توان یک مشکل اساسی قلمداد کرد. چرا که، اولویت‌بندی دقیق حملات در شبکه به‌واسطه آن ممکن نخواهد بود.

در این مقاله تلاش شده است با تغییر سیاست‌های CVSS در ارزیابی تاثیر رخداد حمله بر روی سه پارامتر محرمانگی، صحت داده‌ها و دسترسی‌پذیری، گستره امتیازات بهبود و در نتیجه ارزیابی خطر با دقت بالاتری انجام شود.

از آنجایی که حملات واقعی در شبکه‌های کامپیوتری حملات چند مرحله‌ای هستند، قصد داریم در آینده سیستم پیشنهادی را برای ارزیابی خطر حملات چند مرحله‌ای توسعه بدهیم.

مراجع

[1] H. Joh and Y. K. Malaiya, "Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics," Proc. Int. Conference on Security and Management (SAM11), 2011, pp.10-16.

[2] http://www.first.org/cvss/ (accessed May, 28, 2018)

[3] http://cwe.mitre.org/(accessed May, 28, 2018)

[4] M. Keramati, H. Asgharian, A. Akbari, "Cost-Aware Network Immunization Framework for Intrusion Prevention "International Conference on Computer Applications and Industrial Electronics, pp. 321-326, 2011

[5] M. Keramati, M. Keramati, "Novel Security Metrics for Ranking Vulnerabilities in Computer Networks", 7'th International Symposium on Telecommunications (IST'2014),pp.883 - 888,2014

[6] M. Keramati, "New Vulnerability Scoring System for dynamic security evaluation," 2016 8th International

Symposium on Telecommunications (IST), Tehran, 2016, pp. 746-751.
[7] M.Keramati, "A Novel System for Quantifying the Danger Degree of Computer Network Attacks", 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI) Dec. 22th, 2017. , pp. 804-809.
[8] https://technet.microsoft.com/enus/security/cc998259.aspx, Microsoft Security Center, May 2018.
[9] http://www.symantec.com/security_response/landing/vulnerabilities.jsp, Symantec Vulnerability Scoring System, May 2018.
[10] https://access.redhat.com/security/security-updates/#/, Redhat Vulnerability Scoring System, May 2018.
[11] Wang, Y., & Yang, Y. PVL: A Novel Metric for Single Vulnerability Rating and Its Application in IMS. Journal of Computational Information Systems, 8(2), 579-590, 2012.
[12] Frühwirth, C. & Männistö, T. Improving CVSS-based vulnerability prioritization and response with context information. Proceeedings of International Workshop on Security Measurement and Metrics (MetriSec), 2009, PP. 535-544.
[13] GALLON, L. Vulnerability discrimination using cvss framework. In New Technologies, Mobility and Security (NTMS), 4th IFIP International Conference, 2010, pp. 1 – 6
[14] Spanos, G. & Sioziou, A. & Angelis L. WIVSS: a new methodology for scoring information systems vulnerabilities. Panhellenic Conference on Informatics.2013, PP. 83-90
[15] http://cve.mitre.org/.(accessed May, 7, 2018)
[16] Thaier Hamid, Carsten Maple and Paul Sant. Article: Methodologies to Develop Quantitative Risk Evaluation Metrics. International Journal of Computer Applications 48(14):17-24, June 2012.

.