فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

Fall 2021, 2 (3), 13-23
DOR: 20.1001.1.27832570.1400.2.1.1.2

Received: 20 July 2021
Accepted: 05 Sep 2021

Strategic, Tactical, Technical, and Operational Requirements of Executive Organizations for Developing Cyber Security Vulnerability Calculator

Iman Rajabizadeh[1], Nasser Modiri[2*]

1.MSc Student, Faculty of Electrical and Computer Engineering, North Tehran Branch. Islamic Azad University, Tehran, Iran. iman.rajabizade74@gmail.com

2. Assistant Professor, Faculty of Electrical and Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan Iran. (*Corresponding Author*) nassermodiri@yahoo.com

Abstract

Introduction: Vulnerability analysis is of particular importance as a point of entry into the system and gaining unauthorized access by the attacker. As a result, one of the basic steps in creating the security of organizations is to be aware of the vulnerabilities in information technology systems and planning to fix these vulnerabilities. Also, one of the most important indicators of cyber security is the existence of an organizational gem (coordinated incident response groups) in the executive bodies of the country, which is responsible for preventing, dealing with, and dealing with all security incidents that occur in the space of information production and exchange. One of the requirements for creating an organizational gem in executive bodies is to have a vulnerability management unit and as a result, the existence of a deficiency calculator.

Method: In order to adapt the CIS security controller, we cover this issue by applying two new variables in the basic and environmental criteria of CVSS. These criteria are as follows: the amount of time it takes to detect unauthorized access resulting from a vulnerability in the network and the amount of time it takes to block detected unauthorized access.

Findings: In this article. in order to more accurately assess the severity of the vulnerabilities in the environment, the third version of the conventional vulnerability scoring system (CVSS) according to one of the critical components in cyber defense, i.e. the duration of vulnerability detection and cutting off the unauthorized access resulting from them was developed, and then the performance of the tool was evaluated by examining the vulnerability severity of CVE-2019-1690 and CVE-2019-1758 in order to evaluate the impact and performance of the first controller. The results show the proposed metrics lead to higher performance.

Discussion: The developed CVSS tool is capable of more accurate evaluation of vulnerabilities and providing a suitable score according to the most important CIS control, i.e. creation and management of authorized and unauthorized equipment warehouse. Using the proposed tool Organizations can limit and effectively correct cyber threats more quickly. The proposed method is able to reduce the existing challenges in the field of cyber security of organizations.

Keywords: Vulnerability Assessment, Cyber Threats, Effective Cyber Defense

فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

الزامات راهبردی، تاکتیکی، تکنیکی و عملیاتی دستگاه‌های اجرایی برای توسعه محاسبه‌گر کاستی‌های امنیت سایبری

تاریخ دریافت: ۱٤۰۰/۰٤/۲۹
تاریخ پذیرش:۱٤۰۰/۰٦/۱٤

سال دوم، پاییز ۱٤۰۰
شمارهٔ سوم، صص: ۱۳- ۲۳

ایمان رجبی‌زاده[۱]، ناصر مدیری[۲]*

۱. دانشجوی کارشناسی ارشد، دانشکده مهندسی برق و کامپیوتر، واحد تهران شمال، دانشگاه ازاد اسلامی تهران، ایران.
iman.rajabizade74@gmail.com
۲. استادیار، دانشکده مهندسی برق و کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران. (نویسندهٔ مسئول) nassermodiri@yahoo.com

چکیده: در سال‌های اخیر، مدیریت امنیت سیستم‌های اطلاعاتی و تحلیل مخاطرات امنیتی این سیستم‌ها در سطح گسترده‌ای مورد توجه بوده است. پژوهشگران تلاش‌کرده‌اند نوعی از معیارهای امنیتی را ارائه‌دهند که در تحلیل ایمنی سیستم‌ها، مفید و کاربردی باشند. معیارهای امنیتی امکان اولویت‌بندی مخاطرات پیش روی سیستم را فراهم‌می‌کنند. دراین‌میان تحلیل آسیب‌پذیری‌ها به‌عنوان نقطه ورود به سیستم و کسب دسترسی‌های غیرمجاز توسط مهاجم، اهمیت ویژه‌ای دارد. در نتیجه یکی از گام‌های اساسی در ایجاد امنیت سازمان‌ها آگاهی از آسیب‌پذیری‌های موجود در سیستم‌های فناوری اطلاعات و برنامه‌ریزی جهت رفع این آسیب‌پذیری‌ها می‌باشد. در این مقاله به منظور توسعه و افزایش دقت این سیستم امتیازدهی CVSS با توجه به موثرترین کنترلری که برای دفاع موثر سایبری توسط مرکز امنیت اینترنت (CIS) ارائه‌شده، با افزودن دو معیار جدید تحت عنوان‌های مدت زمان شناسایی و مدت زمان قطع دسترسی غیر مجاز در معیارهای پایه و محیطی اقدام به توسعه و متناسب‌سازی این ابزار شده‌است تا به این صورت با تمرکز بیشتری بر روی سرعت شناسایی دستگاه‌ها و دسترسی‌های غیرمجاز در سازمان‌ها به اولویت‌دهی و بررسی شدت آسیب‌پذیری‌ها و تأثیرات مخرب آن بر روی منافع سازمان پرداخته‌شود.

واژه‌های کلیدی: ارزیابی آسیب‌پذیری، تهدیدات سایبری ، دفاع موثر سایبری.

۱. مقدمه

گسترش سریع اینترنت بسیاری از مسائل امنیت شبکه همچون نشت اطلاعات شخصی، حملات هکرها و ویروس‌های تهدیدآمیز (بدون امضا) را به همراه داشته‌است و موضوع امنیت سایبری مسأله مهم قرن بیست و یکم شده‌است. مسائلی همچون طغیان جنگ سایبری، نیازهای امنیت شبکه را بیش از پیش تهییج‌کرده‌است و ارزیابی وضعیت امنیت سایبری برای رفع کارآمد این قبیل مشکلات امنیتی بسیار ضروری است.

اتحادیه بین‌المللی مخابرات، اولین نسخه از راهنمای راهبرد امنیت سایبر را در سال ۲۰۰۸ و نسخه اصلاحی این شاخص را برای اندازه‌گیری کمی سطح پیشرفت امنیت سایبری در کشورها طراحی کرده است. هدف نهایی اتحادیه بین‌المللی مخابرات از تهیه این شاخص تقویت فرهنگ جهانی امنیت سایبری است. این شاخص شامل پنج مؤلفهٔ قوانین و مقررات[۱]، اقدامات فنی[۲]، ساختارهای اجرایی و سازمانی[۳]، ظرفیت‌سازی[۴]، همکاری ملی و بین‌المللی[۵] است.

این پنج مؤلفه بنیان شاخص جهانی امنیت سایبری را شکل‌می‌دهند، زیرا اجزاء تشکیل‌دهنده فرهنگ ملی یک کشور در امنیت سایبری‌اند. هدف نهایی اتحادیه بین‌المللی مخابرات از این اقدام، بومی‌سازی و یکپارچه‌سازی امنیت سایبری در مقیاس جهانی می‌باشد. از آنجا که همه کشورها به سمت محیطی شبکه‌ای و دیجیتال در حرکت اند، بومی‌سازی به‌موقع امنیت سایبری می‌تواند زیرساخت‌هایی امن‌تر و منعطف‌تر با قابلیت خود ترمیمی ایجادنماید. شاخص امنیت سایبری از پنج مؤلفه اصلی تشکیل‌شده‌است و هرکدام دارای تعدادی شاخص می‌باشند. با ارزش‌گذاری هریک از این شاخص‌ها می‌توان امتیاز امنیت سایبری هر کشور را به‌دست‌آورد.

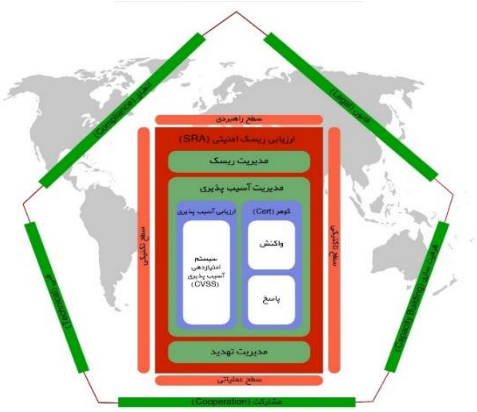
یکی از مهمترین شاخص‌ها در مؤلفه اقدامات فنی، وجود گوهر سازمانی (گروه‌های واکنش هماهنگ رخداد) در دستگاه‌های اجرایی کشور است که وظیفه جلوگیری، رسیدگی و مقابله با کلیه حوادث امنیتی در فضای تولید و تبادل اطلاعات را برعهده دارد. این گروه با نام تیم پاسخ‌گویی سریع به حوادث شبکه‌های رایانه‌ای (CERT[6]) نیز شناخته‌می‌شود. اهداف اصلی ایجاد تیم امداد امنیت رایانه‌ای عبارتند از:

- کاهش و به حداقل رساندن بروز حادثه در شبکه‌های رایانه‌ای
- کاهش و به حداقل رساندن زمان پاسخ به حوادث در حوزه شبکه‌های رایانه‌ای
- کاهش و به حداقل رساندن میزان خسارت حوادث در حوزه شبکه‌های رایانه‌ای

از الزامات ایجاد گوهر سازمانی در دستگاه‌های اجرایی، دارا بودن واحد مدیریت آسیب‌پذیری‌ها و در نتیجه وجود محاسبه‌گر کاستی‌ها است چرا که امروزه ثابت شده‌است که تجهیزات و سرویس‌های موجود در شبکه‌های محلی ضمن اینکه به عنوان ابزاری جهت پیشبرد اهداف کسب و کار سازمان‌ها به‌کارگرفته‌می‌شوند هرکدام دارای برخی نقاط ضعف یا آسیب‌پذیری امنیتی شناخته‌شده و گاه شناخته نشده در برابر تهدیدهای مختلف هستند. این آسیب‌پذیری‌ها می‌تواند مخاطراتی را برای سازمان‌ها به همراه داشته‌باشد. بنابراین سازمان‌هایی که قصد حفظ و امن‌سازی دارایی‌های اطلاعاتی خود را دارند، لازم است این آسیب پذیری‌ها را شناسایی کرده و در جهت رفع آن‌ها برنامه‌ریزی و اقدام‌نمایند. اهمیت کنترل آسیب‌پذیری‌های فنی تجهیزات و سرویس‌های شبکه‌های محلی به‌حدّی است که به عنوان یکی از مهمترین الزامات استاندارد ایزو ۲۷۰۰۱ (کنترل A.12.6.1) در پیاده‌سازی سیستم مدیریت امنیت اطلاعات ISMS[7] نیز مطرح‌شده و باید رعایت‌شود.

روش‌های مختلف ارزیابی آسیب‌پذیری‌ها در حال حاضر وجوددارند اما با برخی محدودیت‌ها همراه هستند. تعیین کیفیت شبکه‌های پیچیده از طریق ارزیابی‌های مبتنی‌بر فرایند تحلیل سلسله مراتبی (AHP) آسان است، اما ارزیابی مبتنی‌بر AHP به علت نفوذ کارشناس آنقدر دقیق نیست. ارزیابی مبتنی‌بر گراف حمله کلیه‌ی حملات بالقوه و واقعی را تشریح‌می‌کند اما مشکل انفجار وضعیت را فرامی‌خواند. ارزیابی‌های مبتنی‌بر CVSS می‌توانند آسیب‌پذیری را امتیازدهی کنند اما رابطه بین آسیب‌پذیری‌های مطرح‌نشده را به‌جای‌می‌گذارند. ارزیابی‌های مبتنی‌بر یادگیری ماشینی بدون نمرهٔ کارشناس دقیق هستند، اما مستلزم نمونه‌های برچسب شده هستند.

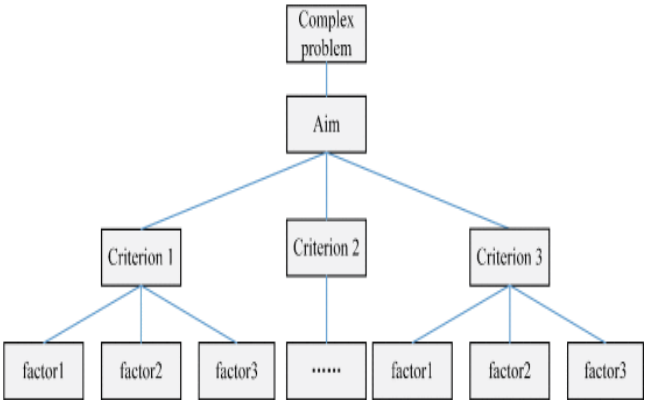
در این مقاله با توجه به اولین و مهمترین کنترلر معرفی‌شده توسط مرکز امنیت اینترنت (CIS[8]) به توسعه معیارهای موجود در سیستم امتیازدهی آسیب‌پذیری عام (CVSS[9]) و ایجاد این ابزار نوآورانه می‌پردازیم که به‌واسطه آن می‌توانیم دقیق‌تر و با تمرکز بر روی مهمترین کنترلر امنیتی معرفی‌شده توسط مرکز امنیت اینترنت (CIS) یعنی شناسایی تجهیزات و دسترسی‌های غیرمجاز، فعالانه به ارزیابی و بررسی شدت آسیب‌پذیری‌ها و مقابله با کلیدی‌ترین مرحله از زنجیره کشت سایبری[10] بپردازیم.



شکل ۱: چارچوب معماری امنیت سایبر

۲. پیشینهٔ پژوهش

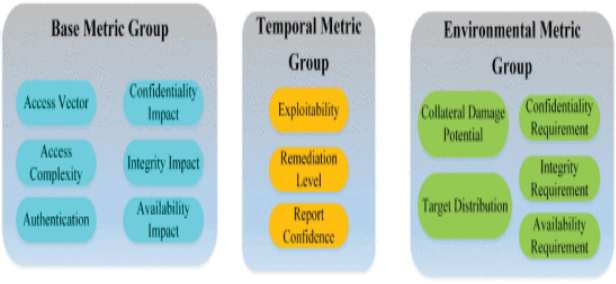
در این بخش به بررسی کارهای انجام‌شده در زمینه ارزیابی ریسک و همچنین ارزیابی آسیب‌پذیری‌های موجود در شبکه خواهیم‌پرداخت. تاکنون مطالعات بسیاری به منظور ارائهٔ روش‌های ارزیابی و محاسبهٔ کمی آسیب‌پذیری‌ها انجام شده‌است که هرکدام مزیت‌ها و محدودیت‌هایی دارند. فرایند تحلیلی سلسله‌مراتبی (AHP) روش تحلیل تصمیم وزنی سلسله‌مراتبی است که توسط ساتی[۱۱] در دهه ۱۹۷۰ مطرح‌شد . تعیین کیفیت مسائل تصمیم پیچیده از طریق تجزیه آن‌ها آسان است (همان‌طور که در شکل ۲ آمده‌است).



شکل ۲: ساختار تحلیل سلسله مراتبی

فرآیند تحلیل سلسله مراتبی روشی آسان و معتبر در حل مسائل تصمیم پیچیده است، اما این فرآیندها ذهن‌گرا و نادرست هستند. هوانگ[۱۲] و همکاران به‌منظور کاهش ذهن‌گرایی، ماتریس داوری وزنی شاخص مبتنی بر نظریه فازی را بهبود دادند و روش جدید تعیین وزن را مطرح‌کردند . چاترجی[۱۳] ریاضیات فازی را برای بهبود AHP معرفی‌کرد که ذهن‌گرایی را کاهش‌داد . فرآیند بهبودیافته تحلیل سلسله‌مراتبی از ذهن‌گرایی کاهیده برخوردار است اما همچنان نفوذ کارشناس وجوددارد.

CVSS استاندارد صنعتی بین‌المللی در ارزیابی آسیب‌پذیری‌های شبکه است. این استاندارد توسط انستیتوی ملی استانداردها و فناوری‌ها (NIST[14]) ایجاد شد و از سوی انجمن پاسخ به حادثه و تیم‌های امنیتی (FIRST[15]) حمایت شده‌است. CVSS از سه گروه تشکیل‌شده‌است (یعنی مبنا، زمانی و محیطی) و هریک شامل مجموعه‌ای از ماتریس‌ها است که در شکل ۳ مشاهده می‌شود.



شکل ۳: گروه ماتریس‌های CVSS

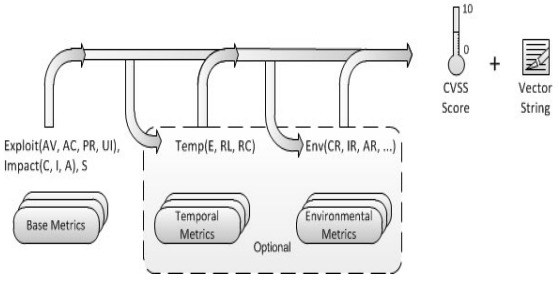
تمرکز CVSS صرفاً روی امتیاز آسیب‌پذیری بدون درنظرگرفتن روابط بین آسیب‌پذیری‌ها است. Yuqing Z و همکاران AHP را به‌منظور بهبود CVSS معرفی‌کردند. مدیری و سعیدی یک رویکرد استاندارد و کاربردی جهت ارزیابی آسیب‌پذیری‌های فنی امنیتی شبکه‌های محلی و تجهیزات و سیستم‌ها و نرم‌افزارهای موجود در این شبکه‌ها را ارائه‌کردند و سپس نتایج استفاده از این رویکرد را در یک شبکه یکپارچه توصیف‌کردند. XiaolinZhao و همکاران مدل چند لایه، چند بُعدی و چند دانه‌ای ارزیابی امنیت شبکه مبتنی‌بر تحلیل AHP ، CVSS و گراف حمله را مطرح‌کردند. شمار روش‌های ارزیابی امنیت شبکه مبتنی‌بر یادگیری ماشینی با خیزش یادگیری ماشینی رو به افزایش است. یادگیری ماشینی، فرآیند جستجوی خودکار الگوها از بی‌شمار داده‌است. AzwarHassan و همکاران تشخیص نفوذ را با کمک روش‌های یادگیری ماشینی، داده‌کاوی و مجموعه داده‌های موثق KDD99 و ISC2012 بررسی کردند.

Gu Y و همکاران مدل تشخیص محروم‌سازی از سرویس (DDoS) را مبتنی‌بر الگوریتم داده‌کاوی مطرح‌کردند.

۱،۲. سیستم امتیازدهی آسیب‌پذیری متعارف

سیستم امتیازدهی آسیب‌پذیری عام CVSS یک چارچوب باز برای ارتباط ویژگی‌ها و میزان آسیب‌پذیری‌های نرم‌افزاری است. این سیستم از سه گروه معیاری پایه[۱۶]، موقتی[۱۷] و محیطی[۱۸] تشکیل‌شده که هرکدام شامل مجموعه ای از معیارها هستند.

معیارهای پایه‌ای، ویژگی‌های اصلی و پایه‌ای یک آسیب‌پذیری هستند که درطول زمان ثابت بوده و به محیط کاربر بستگی ندارند. در مقابل، معیارهای موقتی با گذشت زمان تغییرمی‌کنند، ولی بین محیط‌های کاربری مختلف یکسان هستند. معیارهای محیطی نیز به یک محیط خاص کاربری مربوط بوده و منحصر به آن محیط می‌باشند. از ویژگی‌های روش CVSS سادگی و سهولت درک آن است. در این روش، وقتی به معیارهای پایه‌ای مقادیر مناسبی اختصاص داده‌شود، معادله پایه‌ای، مقداری بین ۰ تا ۱۰ خواهدگرفت. استفاده از معیارهای موقتی و محیطی اختیاری است، ولی می‌توان با تخصیص مقادیر مناسب به این معیارها امتیاز پایه را پالایش‌کرد. استفاده از معیارهای موقتی و محیطی میزان ریسک ناشی از آسیب‌پذیری را با دقت بیشتری منعکس‌می‌سازد، اما استفاده از این معیارها الزامی نیست و با توجه به هدف، ممکن است استفاده از امتیاز پایه کافی باشد.



شکل ۴: فرآیند امتیازدهی CVSS

۲،۲. بهبود و توسعه نسخه ۳ سیستم امتیازدهی آسیب‌پذیری متعارف CVSS

موثرترین و کلیدی‌ترین کنترلری که برای دفاع مؤثر سایبری توسط مرکز امنیت اینترنت (CIS) ارائه شده ،کنترلر اول یعنی تهیه و مدیریت انباره‌ای از تجهیزات و دسترسی‌های مجاز و غیرمجاز می‌باشد که طبق این کنترلر تمامی تجهیزات و دسترسی‌ها در سطح شبکه باید به گونه‌ای شناسایی، پایش و مدیریت شوند که تنها به افراد و تجهیزات مجاز اجازه دسترسی داده‌شود و به این صورت از دسترسی‌های غیرمجاز در سطح شبکه جلوگیری‌شود.

این کنترلر برای سازمان‌ها اهمیت زیادی دارد چرا که نفوذگران در نقاط مختلف دنیا پیوسته در حال جستجو برای یافتن سیستم‌های جدید و تجهیزات آسیب‌پذیر متصل به اینترنت می‌باشند. لپتاپ‌هایی که به‌صورت دوره‌ای به شبکه سازمان متصل‌می‌شوند و دارای آسیب‌پذیری بوده و یا تجهیزات جدیدی که در پایان ساعت کاری سازمان به شبکه متصل‌شده و آسیب‌پذیری‌های آن‌ها تا روز بعد وصل‌نمی‌شوند اهداف مورد علاقه نفوذگران هستند. حتی تجهیزات غیرقابل ردیابی در اینترنت نیز توسط نفوذگرانی که موفق به دسترسی به شبکه داخلی سازمان شده‌اند و به‌دنبال گسترش نفوذ خود می‌باشند، در معرض خطرند. همچنین ابزارهای دیگری مانند سیستم‌های کنفرانس تصویری، سیستم‌های موقت و آزمایشی و شبکه‌های مهمان باید به‌دقت مدیریت‌شده و یا ایزوله شوند تا از حمله نفوذگران از این طریق به شبکه سازمان جلوگیری‌شود. در صورت استفاده سازمان از فناوری BYOD[19] (که کاربران قادرند تجهیزات خانگی و شخصی خود را به شبکه سازمان متصل‌نمایند) باید توجه‌کرد که در صورت آلوده‌بودن این تجهیزات کل شبکه سازمان در معرض خطر قرارخواهدگرفت. همچنین کنترل و مدیریت تمامی تجهیزات متصل به شبکه سازمان نقشی حیاتی در پیاده‌سازی و اجرای سیستم‌های پشتیبان و بازیابی خواهدداشت.

با توجه به اهمیت بالای این کنترلر و نبود معیار مرتبط با این موضوع در معیارهای سیستم امتیازدهی متعارف (CVSS)، در این مقاله به منظور متناسب‌سازی سیستم امتیازدهی CVSS این مسئله را با اعمال دو متغیر جدید تحت عنوان‌های مدت زمان شناسایی و مدت زمان قطع دسترسی غیرمجاز در معیارهای پایه و محیطی CVSS پوشش می‌دهیم. این معیارها به شرح زیر می‌باشد:

۱،۲،۲. مدت زمان شناسایی (Reconnaissance Duration)

این معیار مدت زمانی که طول می‌کشد تا دسترسی غیرمجاز حاصل از یک آسیب‌پذیری در شبکه را شناسایی‌کنیم توصیف‌می‌کند. در این معیار هرچه مدت زمان سپری‌شده برای شناسایی دسترسی غیرمجاز در شبکه بیشتر باشد مقدار متریک بزرگ‌تر خواهدبود و در نتیجه ریسک بیشتری را به همراه خواهدداشت. مدت زمان شناسایی با توجه به ماهیت آسیب‌پذیری‌ها و روشی که از آسیب‌پذیری‌ها سوءاستفاده می‌شود، می‌تواند در هر نوع آسیب‌پذیری متفاوت باشد.

۲،۲،۲. مدت زمان قطع دسترسی غیرمجاز (Denial Access Duration)

پس از شناسایی دسترسی غیرمجاز در شبکه این معیار مدت زمانی را که طول می‌کشد تا دسترسی غیرمجاز شناسایی‌شده را مسدودکنیم توصیف‌می‌کند. در این معیار هرچه مدت زمان سپری‌شده جهت مسدود سازی دسترسی غیرمجاز در شبکه بیشتر باشد مقدار متریک بزرگتر خواهدبود و در نتیجه ریسک بیشتری را به همراه خواهدداشت. مدت زمان مسدودسازی دسترسی غیرمجاز با توجه به ماهیت آسیب‌پذیری‌ها و روشی که از آسیب‌پذیری‌ها سوءاستفاده می‌شود می‌تواند در هر نوع آسیب‌پذیری متفاوت باشد.

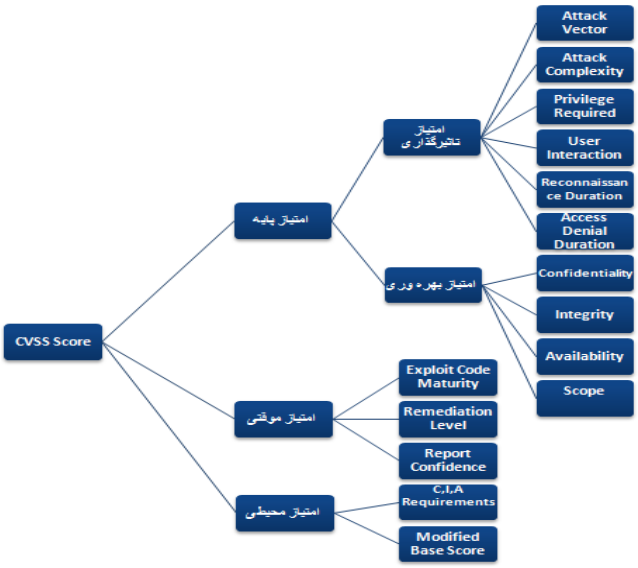
همچنین در ابزار توسعه داده‌شده دو معیار Modified Reconnaissance Duration, Modified Access Denial Duration نیز در قسمت معیارهای محیطی اضافه شده‌است که این معیارها تحلیلگر را قادرمی‌سازند تا معیارهای پایه را طبق تغییراتی که در محیط تحلیلگر وجوددارد، تنظیم‌کند. اکنون این ابزار در آدرس https://cve-calculator.ir در دسترس و قابل بهره‌برداری می‌باشد.

لیست مقادیر احتمالی و سطوح این مقدارها به صورت جدول زیر شرح داده می‌شود.

تمامی مشخصه‌ها و مقادیر کمی شرح داده شده برمبنای مدل CVSS می‌باشد.

معیار های پایه جدید	مقدار متریک	توصیف	مقدار کمی
مدت زمان شناسایی	تعریف نشده(X)	اختصاص دادن این مقدار به معیار روی امتیاز تأثیر نمی گذارد. این یک سیگنال برای یک معادله امتیازدهی است تا از این معیار رد شود.	1
	زیاد(H)	این مقدار در شرایطی که مدت زمان شناسایی دستگاه یا دسترسی غیر مجاز در شبکه بیش از 10080 دقیقه (یک هفته) طول بکشد به معیار اختصاص داده می شود.	1.5
	متوسط (M)	این مقدار در شرایطی که مدت زمان شناسایی دستگاه یا دسترسی غیر مجاز در شبکه حدود 1440 دقیقه (یک روز) طول بکشد به معیار اختصاص داده می شود.	1
	کم (L)	این مقدار در شرایطی که مدت زمان شناسایی دستگاه یا دسترسی غیر مجاز در شبکه کمتر از 60 دقیقه طول بکشد به معیار اختصاص داده می شود.	0.5
مدت زمان قطع دسترسی غیر مجاز	تعریف نشده(X)	اختصاص دادن این مقدار به معیار روی امتیاز تأثیر نمی گذارد. این یک سیگنال برای یک معادله امتیازدهی است تا از این معیار رد شود.	1
	زیاد(H)	پس از شناسایی دسترسی غیر مجاز، این مقدار در شرایطی که مدت زمان قطع دستگاه یا دسترسی غیر مجاز در شبکه بیش از 10080 دقیقه (یک هفته) طول بکشد به معیار اختصاص داده می شود.	1.5
	متوسط (M)	پس از شناسایی دسترسی غیر مجاز، این مقدار در شرایطی که مدت زمان قطع دستگاه یا دسترسی غیر مجاز در شبکه حدود 1440 دقیقه (یک روز) طول بکشد به معیار اختصاص داده می شود.	1
	کم (L)	پس از شناسایی دسترسی غیر مجاز، این مقدار در شرایطی که مدت زمان قطع دستگاه یا دسترسی غیر مجاز در شبکه کمتر از 60 دقیقه طول بکشد به معیار اختصاص داده می شود.	0.5

جدول۱: معیارهای پایه‌های جدید



شکل ۵: معیارهای سیستم CVSS توسعه‌یافته

۳،۲. مقیاس امتیازدهی شدت کیفی:

برای بعضی از هدف‌ها مفید است که یک نمایش متنی از امتیازات عددی پایه، موقتی و محیطی داشته باشیم. تمامی امتیازات را می‌توان به صورت یک رتبه‌بندی کیفی که در جدول زیر تعریف شده، نشان‌داد.

رتبه بندی	امتیاز CVSS
هیچ	۰،۰
کم	۰،۱ – ۳،۹
متوسط	۴،۰ – ۶،۹
زیاد	۷،۰ – ۸،۹
بحرانی	۹،۰ – ۱۰

جدول ۲: مقیاس امتیازدهی شدت کیفی

به‌عنوان مثال ، یک امتیاز پایه CVSS برابر۴ دارای درجه شدت متوسط می‌باشد . استفاده از این نوع امتیازدهی کیفی اختیاری است و هیچ نیازی به ثبت ان‌ها هنگام انتشار امتیازات CVSS نمی‌باشد. این امتیازها برای کمک به سازمان‌ها در ارزیابی و اولویت‌بندی صحیح فرآیندهای مدیریت آسیب‌پذیری خود درنظر گرفته‌شده‌اند.

۴،۲.معادلات CVSS توسعه‌یافته

معادلات CVSS توسعه یافته در این مقاله به شرح زیر می‌باشد:

معادله پایه:

امتیاز پایه تابعی از معادلات مربوط به امتیازهای تأثیرگذاری و قابلیت بهره‌وری هستند. امتیاز پایه ابزار CVSS معرفی‌شده در این مقاله به صورت زیر تعریف‌می‌شود:

If (Impact sub score <= 0) 0 else,
Scope Unchanged[4]
$Roundup(Minimum[(Impact+Exploitability), 10])$
Scope Changed
$Roundup(Minimum[1.08\times(Impact+Exploitability), 10])$

و امتیاز تأثیرگذاری (ISC)[۲۰] به شکل زیر تعریف‌می‌گردد:

Scope Unchanged $6.42 \times ISC_{Base}$
Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

که در این معادله:

$$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$$

و امتیاز قابلیت بهره‌وری برابر است با:

$8.22 \times AttackVector \times AttackComplexity \times privilegeRequired \times UserInteraction \times$ ReconnaissanceDuration × AccessDenialDuration

معادله موقتی:

امتیاز موقتی به شکل زیر تعریف می‌شود:

$Roundup(BaseScore\ ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$

معادله محیطی:

امتیاز محیطی ابزار CVSS معرفی شده در این مقاله نیز به شکل زیر تعریف می‌شود:

If (Modified Impact Sub score <= 0) 0 else,
If Modified Scope is Unchanged:
Round up (Round up (Minimum [(M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Rememediation Level × Report Confidence)
If modified Scope is Changed:
Round up (Round up (Minimum [1.08 × (M.Impa M Impact+ M.Exploitability) ,10]) × Exploit Code MatCode Maturity × Remediation Level × Report Confidence)

و امتیاز تأثیرگذاری اصلاح شده به صورت زیر تعریف می‌شود:

If Modified Scope is Unchanged: $6.42 \times [ISCModified]$
If Modified Scope is Changed:

$7.52 \times [ISCModified - 0.029]$-3.25× $[ISCModified - 0.02]^{15}$

که در این معادله:

$$ISC_{Modified} = Minimum\ [[1 - (1 - M.IConf \times CR) \times (1 - M.IInteg \times IR) \times (1 - M.IAvail \times AR)], 0.915]$$

امتیاز قابلیت بهره‌وری اصلاح شده نیز برابر است با:

$$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction \times M.ReconnaissanceDuration \times M.AccessDenialDuration$$

۳. تجزیه تحلیل روش پیشنهادی

اکنون به منظور ارزیابی ابزار بهبودیافته به ارزیابی شدت آسیب‌پذیری های شناسایی‌شده با استفاده از ورژن ۳ از سیستم امتیازدهی آسیب پذیری عام و مقایسه آن با ماشین حساب توسعه‌داده شده CVSS می-پردازیم.

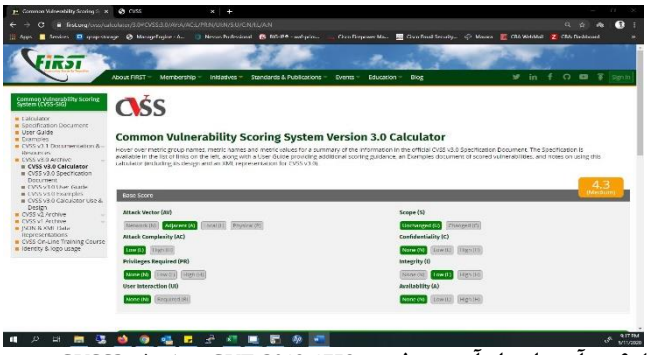
۱،۳. آسیب پذیری CVE-2019-1758

در سوئیچ‌های سیسکو سری Catalyst6500 این آسیب‌پذیری که بر روی عملکرد پروتکل 802.1x در نرم‌افزار IOS این سوئیچ‌ها تأثیرمی-گذارد می‌تواند به مهاجم غیرمجاز مجاور اجازه‌دهد تا قبل از تأیید هویت به شبکه دسترسی پیدا کند. یک مهاجم می‌تواند با تلاش برای اتصال به شبکه در پورت پیکربندی‌شده 802.1x از این آسیب‌پذیری سوءاستفاده کند و یک بهره‌برداری موفق می‌تواند به مهاجم اجازهدهد تا به‌طور متناوب به شبکه دسترسی پیداکند. متریک‌های این آسیب‌پذیری به شرح زیر می‌باشد:

Metric	Value	Comments
Attack Vector	مجاور(A)	بهره برداری از این آسیب پذیری نیاز به مجاورت شبکه با سیستم هدف دارد.
Attack Complexity	کم (L)	پیچیدگی در ساخت بسته های 802.1x برای بهره برداری از آسیب پذیری کم است.
Privileges Required	هیچ (N)	مهاجم قبل از حمله غیر مجاز بوده و به همین دلیل هیچ نیازی به دسترسی به تنظیمات برای انجام حمله ندارد.
User Interaction	هیچ (N)	سیستم آسیب پذیر می تواند بدون تعامل با کاربر مورد بهره وری قرار گیرد.
Scope	بدون تغییر (U)	این آسیب پذیری موجب دور زدن تایید هویت می شود اما تأثیر در محدوده اصلی مؤلفه آسیب پذیر موجود می باشد.
Confidentiality Impact	هیچ (N)	هرگونه تأثیر محرمانه بودن ، تأثیر ثانویه است.
Integrity Impact	کم (L)	اصلاح داده ها امکان پذیر است، اما مهاجم کنترلی روی عواقب یک اصلاح ندارد واصلاح داده ها تأثیر مستقیم و جدی ای بر جزء تأثیریافته ندارد.
Availability Impact	هیچ (N)	هیچ تأثیری روی قابلیت دسترسی در جزء تأثیریافته وجود ندارد.

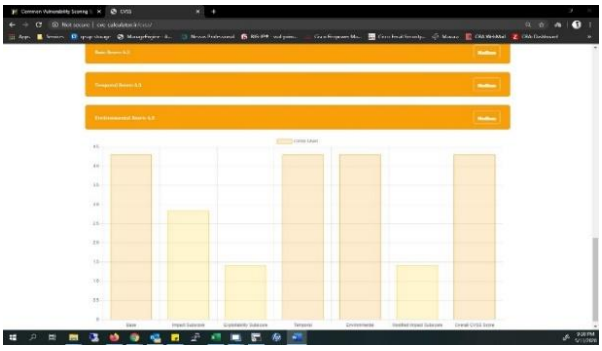
جدول ۳:متریک های اسیب پذیری CVE-2019-1758

با واردکردن مقادیر بالا در ابزار ارائه شده توسط موسسه FIRST، امتیاز و شدت آسیب‌پذیری برابر ۴،۳ (متوسط) محاسبه‌می‌گردد:



شکل۶ :برآورد امتیاز آسیب پذیری CVE-2019-1758 در نسخهCVSS3

در صورتی که به‌منظور صحه‌سنجی ابزار توسعه داده‌شده مقادیر بالا را بدون در نظرگرفتن دو عامل جدید در این ماشین حساب واردکنیم، مجددا امتیاز این آسیب‌پذیری برابر با ۴،۳ (متوسط) به‌دست می‌آید.



شکل ۷ : براورد امتیازآسیب پذیری CVE-2019-1758

حال در صورتی که زیرساخت مناسب برای تشخیص سریع آسیب‌پذیری‌ها و وصله‌کردن آن آسیب‌پذیری در کوتاه‌ترین زمان ممکن وجود داشته‌باشد می‌توانیم دسترسی‌های غیرمجاز را در کوتاه‌ترین زمان شناسایی و از فعالیت آن جلوگیری-نماییم.

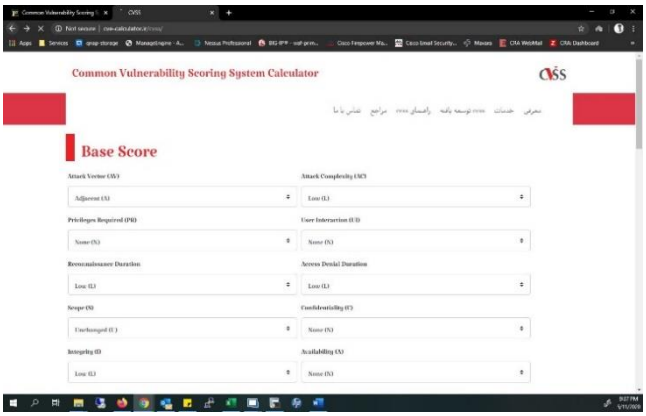
Metric	Value	Comments
Attack Vector	مجاور(A)	بهره برداری از این آسیب پذیری نیاز به مجاورت شبکه با سیستم هدف دارد.
Attack Complexity	کم (L)	پیچیدگی در ساخت بسته های 802.1x برای بهره برداری از آسیب پذیری کم است.
Privileges Required	هیچ (N)	مهاجم قبل از حمله غیر مجاز بوده و به همین دلیل هیچ نیازی به دسترسی به تنظیمات برای انجام حمله ندارد.
User Interaction	هیچ (N)	سیستم آسیب پذیر می تواند بدون تعامل با کاربر مورد بهره وری قرار گیرد.
Scope	بدون تغییر (U)	این آسیب پذیری موجب دور زدن تایید هویت می شود اما تأثیر در محدوده اصلی مؤلفه آسیب پذیر موجود می باشد.
Confidentiality Impact	هیچ (N)	هرگونه تأثیر محرمانه بودن ، تأثیر ثانویه است.
Integrity Impact	کم (L)	اصلاح داده ها امکان پذیر است، اما مهاجم کنترلی روی عواقب یک اصلاح ندارد واصلاح داده ها تأثیر مستقیم و جدی ای بر جزء تأثیریافته ندارد.
Availability Impact	هیچ (N)	هیچ تأثیری روی قابلیت دسترسی در جزء تأثیریافته وجود ندارد.
Reconnaissance Duration	کم (L)	با توجه به وجود زیر ساخت مناسب شناسایی دسترسی غیر مجاز در کمتر از 60 دقیقه انجام می شود.
Access Denial Duration	کم (L)	پس از شناسایی در مدت زمان کمتر از 60 دقیقه قادر به قطع دسترسی غیر مجاز هستیم.

جدول۴:متریک‌های اسیب پذیری CVE-2019-1758 با احتساب دو معیار جدید

در ماشین حساب توسعه داده‌شده تأثیر وجود این زیرساخت با دو وکتور سرعت شناسایی دسترسی‌های غیرمجاز و مدت زمان قطع آن دسترسی محاسبه‌می‌گردد.

با واردکردن متریک‌های جدول ۴ در ابزار توسعه یافته امتیاز و شدت آسیب‌پذیری از ۴,۳(متوسط) به ۲,۲ و ریسک کم تغییرمی‌کند و به این صورت در این ابزار با توجه به مدت زمان شناسایی و سرعت قطع دسترسی غیر مجاز که یکی از مهمترین مؤلفه‌ها در دفاع سایبری می‌باشد امتیاز دقیق‌تری نسبت به ابزار ارائه شده توسط موسسه First خواهیم داشت. این کاهش امتیاز نشان‌دهنده اهمیت وجود زیرساختی جهت مدیریت و شناسایی دسترسی‌های غیرمجاز می‌باشد زیرا در صورتی که آسیب‌پذیری‌ها به سرعت شناسایی‌شده و از دسترسی‌های غیر مجاز حاصل از آن جلوگیری گردد میزان ریسک و تهدید حاصل از آسیب-پذیری به مقدار زیادی کاهش می‌یابد. انتخاب وکتورها و نمودار امتیاز این آسیب‌پذیری در ابزار توسعه داده شده به شرح شکل‌های ۸و۹می-باشد:

شکل۸:امتیاز ابزار توسعه‌یافته آسیب پذیری CVE-2019-1758



شکل ۹:انتخاب ابزار توسعه یافته آسیب پذیری CVE-2019-1758

۲,۳. آسیب‌پذیری CVE-2019-1690

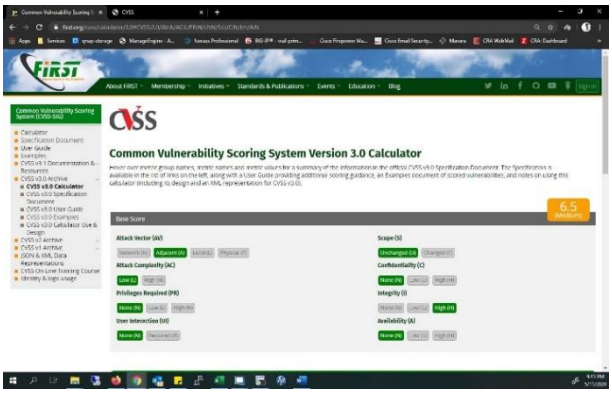
این آسیب‌پذیری بر روی رابط مدیریتی نرم‌افزار CiscoAPIC[21] قرار دارد و در دستگاه‌هایی که دارای نسخه‌های قبل از (۰,۲۱C) ۴,۲ می‌باشد قابل سوءاستفاده می‌باشد . با استفاده از این آسیب‌پذیری یک مهاجم مجاور و غیرمجاز می‌تواند به دستگاه دارای آسیب‌پذیری دسترسی غیرمجاز داشته‌باشد. این آسیب‌پذیری ناشی از عدم وجود مکانیسم‌های مناسب کنترل دسترسی برای اتصالات محلی IPv6 اعمال شده بر روی رابط مدیریتی یک دستگاه دارای آسیب‌پذیری می‌باشد. مهاجم در همان شبکه فیزیکی می‌تواند از این آسیب‌پذیری با تلاش برای اتصال به آدرس پیوند محلی IPv6 در دستگاه آسیب‌پذیر سوءاستفاده‌کند و یک سوء-استفاده موفقیت‌آمیز می‌تواند به مهاجم اجازه‌دهد محدودیت‌های پیش-فرض کنترل دسترسی را بر روی دستگاه مربوطه دور بزند.

متریک‌های این آسیب‌پذیری به شرح جدول۵ می‌باشد.

Metric	Value	Comments
Attack Vector	مجاور(A)	بهره برداری از این آسیب پذیری نیاز به مجاورت شبکه با سیستم هدف دارد
Attack Complexity	کم (L)	شرایط دسترسی خاص یا شرایط تضعیف وجود ندارد و مهاجم می تواند موفقیت قابل تکرار را در برابر هر آسیب پذیر انتظار داشته باشد
Privileges Required	هیچ (N)	مهاجم قبل از حمله غیر مجاز بوده و به همین دلیل هیچ نیازی به دسترسی به تنظیمات برای انجام حمله ندارد
User Interaction	هیچ (N)	سیستم آسیب پذیر می تواند بدون تعامل با کاربر مورد بهره برداری قرار گیرد.
Scope	بدون تغییر (U)	این آسیب پذیری موجب دور زدن تایید هویت می شود اما تأثیر در محدوده امنی مؤلفه آسیب پذیر موجود می باشد
Confidentiality Impact	هیچ (N)	هرگونه تأثیر محرمانه بودن ، تأثیر ناچیز است
Integrity Impact	زیاد (H)	به مهاجم اجازه می دهد تا کنترل کامل سیستم آسیب دیده را به دست بگیرد
Availability Impact	هیچ (N)	هیچ تأثیری روی قابلیت دسترسی در جزء تأثیریافته وجود ندارد

جدول ۵: متریک‌های آسیب‌پذیری CVE – 2019 - 1690

با وارد کردن مقادیر بالا در ابزار ارائه شده توسط موسسه First، امتیاز و شدت آسیب‌پذیری برابر 6.5 (متوسط) محاسبه می‌گردد.



شکل۱۰: برآورد امتیاز آسیب‌پذیری CVE – 2019 - 1690

در صورتی که به منظور صحه‌سنجی ابزار توسعه داده شده مقادیر بالا را بدون درنظرگرفتن دو عامل جدید در این ماشین حساب واردکنیم، مجدداً امتیاز این آسیب‌پذیری برابر با 6.5 (متوسط) به‌دست‌می‌آید.

شکل ۱۱: امتیاز آسیب پذیری CVE – 2019 – 1690 در ابزار توسعه داده شده

حال در صورتی که زیرساخت مناسب برای تشخیص سریع آسیب-پذیری‌ها و وصله کردن آن آسیب‌پذیری در کوتاه‌ترین زمان ممکن وجود نداشته‌باشد و این آسیب‌پذیری پس از گذر زمان زیادی شناسایی و وصله نشود می‌تواند تهدیدی جدی را برای سازمان به‌وجودآورد.

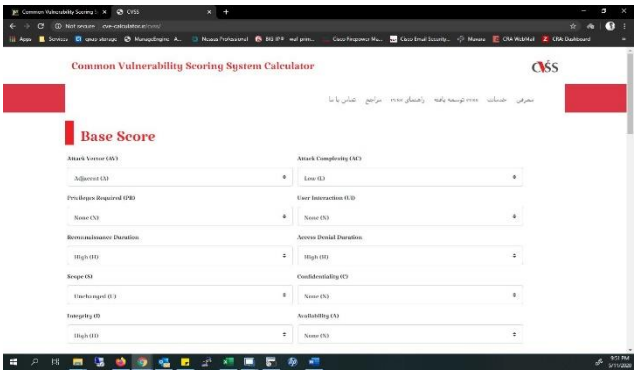
در ماشین حساب توسعه داده‌شده تأثیر عدم وجود این سرور با دو وکتور سرعت شناسایی دسترسی‌های غیرمجاز و مدت زمان قطع آن دسترسی محاسبه‌می‌گردد.

Metric	Value	Comments
Attack Vector	مجاور(A)	بهره برداری از این آسیب پذیری نیاز به مجاورت شبکه با سیستم هدف دارد.
Attack Complexity	کم (L)	شرایط دسترسی خاص یا شرایط تضعیف وجود ندارد و مهاجم می تواند موفقیت قابل تکرار را در برابر جزء آسیب پذیر انتظار داشته باشد.
Privileges Required	هیچ (N)	مهاجم قبل از حمله غیر مجاز بوده و به همین دلیل هیچ نیازی به دسترسی به تنظیمات برای انجام حمله ندارد.
User Interaction	هیچ (N)	سیستم آسیب پذیر می تواند بدون تعامل با کاربر مورد بهره وری قرار گیرد.
Scope	بدون تغییر (U)	این آسیب پذیری موجب دور زدن تایید هویت می شود اما تأثیر در محدوده اصلی مؤلفه آسیب پذیر موجود می باشد.
Confidentiality Impact	هیچ (N)	هرگونه تأثیر محرمانه بودن ، تأثیر ثانویه است.
Integrity Impact	زیاد (H)	به مهاجم اجازه می دهد تا کنترل کامل سیستم آسیب دیده را به دست بگیرد.
Availability Impact	هیچ (N)	هیچ تأثیری روی قابلیت دسترسی در جزء تأثیریافته وجود ندارد.
Reconnaissance Duration	زیاد (H)	با توجه به عدم وجود زیر ساخت مناسب شناسایی دسترسی غیر مجاز ممکن است بیشتر از یک هفته (10080 دقیقه) طول بکشد.
Access Denial Duration	زیاد (H)	با توجه به عدم وجود زیر ساخت مناسب جهت شناسایی دسترسی غیر مجاز ممکن است قطع این دسترسی بیشتر از یک هفته (10080 دقیقه) طول بکشد.

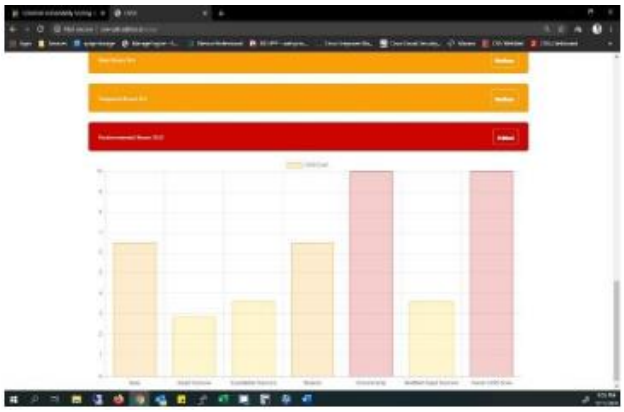
جدول ۶: متریک‌های آسیب پذیری CVE – 2019 – 1690 با احتساب دو متریک جدید

با واردکردن متریک‌های جدول ۶ در ابزار توسعه یافته امتیاز و شدت آسیب‌پذیری از ۶,۵ (متوسط) به ۱۰ و با ریسک بحرانی تغییرمی‌کند و به این صورت می‌توان به اهمیت نقش عامل سرعت شناسایی تجهیزات و دسترسی‌های غیرمجاز در جلوگیری از تهدیدهای سایبری اشاره‌کرد و به این صورت در ابزار توسعه‌داده‌شده ارزیابی دقیق‌تری از شدت این آسیب‌پذیری نسبت به نسخه سوم از CVSS خواهیم‌داشت. با توجه به اینکه این آسیب‌پذیری تأثیر بسیار زیادی در یکپارچگی سیستم دارد، در صورتی که به‌سرعت شناسایی و وصله نشود می‌تواند خسارات جبران-ناپذیری را به سازمان‌ها تحمیل‌کند.

انتخاب‌ها و نمودار امتیاز این آسیب‌پذیری در ابزار توسعه‌داده‌شده به شرح شکل‌های ۱۲و۱۳ می‌باشد:



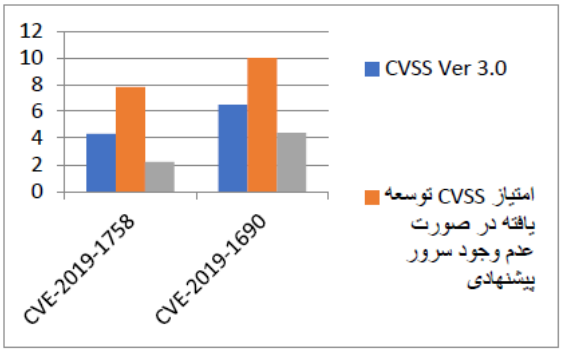
شکل۱۲: انتخاب‌های CVSS توسعه یافته برای آسیب پذیری CVE-2019- 1690



شکل۱۳: امتیاز آسیب پذیری CVE- 2019 -1690 در ابزار توسعه داده شده با معیارجدید

اکنون پس از ارزیابی شدت آسیب‌پذیری‌های ذکرشده، اهمیت ابزار توسعه یافته را می‌توان با بررسی دو عامل سرعت شناسایی دسترسی-های غیرمجاز و سرعت قطع آن دسترسی و همچنین بررسی میزان تأثیر این دو عامل در شدت آسیب‌پذیری‌ها بررسی‌نمود.

نمودار مقایسه امتیاز آسیب‌پذیری‌های بررسی‌شده در نسخه سوم ابزار CVSS با امتیاز ابزار توسعه‌یافته در صورت وجود و عدم وجود زیرساخت مناسب برای شناسایی دستگاه‌ها و دسترسی‌های غیرمجاز شبکه به صورت شکل۱۴ ارائه‌می‌شود:



شکل ۱۴: نمودار مقایسه آسیب پذیری‌های بررسی‌شده درنسخه CVSS ۳ و ابزار توسعه‌یافته

۴. نتیجه‌گیری

در این مقاله به منظور ارزیابی دقیق تر از شدت آسیب‌پذیری‌های موجود در محیط، نسخه سوم از سیستم امتیازدهی آسیب‌پذیری متعارف (CVSS) با توجه به یکی از مؤلفه‌های حیاتی در دفاع سایبری یعنی مدت زمان شناسایی آسیب‌پذیری‌ها توسعه‌داده‌شد و اکنون این ابزار در آدرس https://cve-calculator.ir در دسترس و قابل بهره‌برداری می‌باشد.

در ادامه عملکرد ابزار توسعه‌داده‌شده مورد بررسی و ارزیابی قرارگرفت و نقاط قوت و ضعف آن بیان‌شد. از این ابزار برای امتیازدهی شدت آسیب‌پذیری‌های CVE-2019-1690 و CVE-2019-1758 در جهت ارزیابی میزان تأثیر و عملکرد کنترل اول CIS در برابر تهدیدات سایبری استفاده‌شد. در نهایت با توجه به بررسی و ارزیابی‌های صورت‌گرفته نتایج زیر حاصل‌شد:

- ابزار CVSS توسعه‌داده‌شده، قادر به ارزیابی دقیق‌تر آسیب-پذیری‌ها و ارائه امتیازی متناسب با توجه به مهم‌ترین کنترل CIS یعنی ایجاد و مدیریت انباره تجهیزات مجاز و غیرمجاز می‌باشد.
- دستگاه‌های اجرایی می‌توانند با استفاده از ابزار توسعه‌داده‌شده و با توجه به اهمیت زمان و سرعت شناسایی آسیب‌پذیری‌ها و سرعت وصله‌کردن آسیب‌پذیری‌ها میزان آمادگی و اتکا به شبکه سازمان را در برابر تهدیدات مختلف بسنجند.
- با ارزیابی دقیق‌تر کاستی‌ها توسط محاسبه‌گر توسعه‌داده‌شده، می‌توانیم به صورت موثرتری اقدامات لازم جهت افزایش امنیت سایبری سازمان را اولویت‌دهی کرده و وزن و اهمیت آن را مشخص کنیم.
- با استفاده از ابزار پیشنهادشده سازمان‌ها می‌توانند با سرعت بیشتری به محدودسازی و اصلاح مؤثر تهدیدات سایبری بپردازند.
- روش پیشنهادی قادر است تا چالش‌های موجود در زمینه امنیت سایبری سازمان‌ها را کاهش‌دهد.

۵. پیشنهاد

برای اجرایی و عملیاتی کردن ابزار CVSS در محیط‌های صنعتی همواره با چالش‌هایی همچون مدت زمان شناسایی و اصلاح آسیب‌پذیری ها ، تعداد سیستم‌های آسیب‌پذیر و اندازه شبکه محیط و همچنین نوع فعالیت محیط مورد نظر (فعالیت‌های پیوسته و گسسته) مواجه‌می‌شویم. در این مقاله چالش سرعت شناسایی و اصلاح آسیب‌پذیری‌ها بررسی و برطرف‌شد اما به منظور هوشمندسازی این سیستم و بهره‌وری کامل‌تر از این ابزار در محیط در آینده باید مطالعات بیشتری صورت‌گیرد.

به عنوان کارهای تحقیقاتی آینده که می‌توانند در جهت توسعه ابزار ارائه‌شده در این تحقیق انجام‌شوند، پیشنهادهای زیر مطرح می‌گردد:

- ایجاد و اعمال معیارهایی جهت افزایش دقت ابزار CVSS با توجه به نوع فعالیت (فرآیندهای گسسته و یا مداوم) در محیط‌های صنعتی و سازمانی.
- ایجاد و اعمال پارامترهایی جهت ارزیابی طیفی از آسیب‌پذیری‌ها به منظور مشخص‌نمودن آستانه سازش محیط با تعداد گسترده‌ای از آسیب‌پذیری‌ها.
- ایجاد و به‌کارگیری فرآیندهای ممیزی و راستی‌آزمایی به منظور صحه‌سنجی اعمال به‌روزرسانی جهت رفع آسیب‌پذیری‌ها و برآورد ریسک ناشی از عدم اعمال به‌روزرسانی.
- ایجاد معیارهای افزایش دقت ابزار CVSS با توجه به اندازه شبکه (کوچک، متوسط، بزرگ) و تعداد آسیب‌پذیری‌های موجود در محیط.

مراجع

[۱] مدیری، ناصر (۱۳۹۶). جرم شناسی سایبری(امنیت،مدل سازی تهدیدات وجرم شناسی شبکه). انتشارات مهرگان قلم

[۲] رجبی زاده، ایمان و ناصر مدیری . (۱۳۹۹) . ارائه رویکردی دفاعی برای مقابله با شناسایی تجهیزات فعال شبکه‌های کامپیوتری . پایان نامه کارشناسی ارشد . دانشگاه ازاد اسلامی واحد تهران شمال

[۳] سعیدی، وحید و ناصر مدیری. (۱۳۹۳). ارائه رویکردی جهت ارزیابی آسیب‌پذیری‌های فنی شبکه‌های محلی. دومین همایش ملی پژوهش‌های کاربردی در علوم کامپیوتر و فناوری اطلاعات. تهران. دانشگاه جامع علمی کاربردی.

[۴] سعیدی، وحید و ناصر مدیری(۱۳۹۳). ارائه رویکردی جهت ارزیابی آسیب‌پذیری‌های فنی شبکه‌های محلی. دومین همایش ملی پژوهش‌های کاربردی در علوم کامپیوتر و فناوری اطلاعات. تهران. دانشگاه جامع علمی کاربردی.

[۵] رجبی زاده، ایمان و ناصر مدیری. (۱۳۹۹) . ابزار توسعه یافته امتیازدهی آسیب¬پذیری عام . http://cve-calculator.ir/cvss/

[6] Ramos, A., Lazar, M., Holanda Filho, R., & Rodrigues, J. J. (2017). Model-based quantitative network security metrics:

A survey. IEEE Communications Surveys & Tutorials, 19(4), 2704-2734.
[7] Zhao, X., Zhang, Y., Xue, J., Shan, C., & Liu, Z. (2020). Research on Network Risk Evaluation Method Based on a Differential Manifold. IEEE Access, 8, 66315-66326.
[8] The Center for Internet Cybersecurity: "Critical Security Controls .Version 7.1" . April 1, 2019. Available at: https://www.cisecurity.org/critical-controls.cfm .
[9] Qi, W., Yan, X., Bin, Q., Shuang, L. X., & Hui, Y. (2019, May). A Risk Assessment Method of Intelligent Substation Relay Protection Device Based on Severity Index. In 2019 IEEE 2nd International Conference on Electronics Technology (ICET) (pp. 381-386). IEEE.
[10] Huang, Y., Tao, C., & Wang, Z. Q. (2015). Fuzzy comprehensive evaluation model of computer network security and its application. In Applied Mechanics and Materials (Vol. 711, pp. 286-292). Trans Tech Publications Ltd.
[11] Chatterjee, S., Chaudhuri, B., Bhar, C., & Shukla, A. (2017, December). Estimation of software reliability and development cost using interval type-2 fuzzy AHP. In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS) (pp. 682-688). IEEE.
[12] Kebande, V. R., Kigwana, I., Venter, H. S., Karie, N. M., &Wario, R. D. (2018, August). CVSS Metric-Based Analysis, Classification and Assessment of Computer Network Threats and Vulnerabilities. In 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD) (pp. 1-10). IEEE.
[13] K. Lei and Y. Zhang, "Vulnerability availability quantification evaluation system based on vulnerability", J. Comput. Res. Develop., vol. 54, pp. 2296-2309, Aug. 2017.
[14] ZHAO, X. L., ZHANG, Y. M., YA, H., ZHANG, X. H., & YANG, Y. N. (2017). Multi-Layer, Multi-Dimensional and Multi-Granularity Network Model to Measure Network Security. DEStech Transactions on Computer Science and Engineering, (cimns).
[15] Ray, S. (2019, February). A Quick Review of Machine Learning Algorithms. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 35-39). IEEE.
[16] Ray, S. (2019, February). A Quick Review of Machine Learning Algorithms. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 35-39). IEEE.
[17] Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semi-supervised k-means ddos detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351-64365.
[18] 2017. Common vulnerability scoring system v3.0 specification document 2017 https://www.first.org/cvss/cvss-v30-specification-v1.7.pdf

پی‌نوشت

1. Legal Measures
2. Technical Measures
3. Organizational Measures
4. Capacity Building
5. Cooperation
6. Computer emergency response team
7. The information security management system
8. Center for Internet Security
9. Common Vulnerability Scoring System
10. Cyber killchain
11. Saaty
12. Huang
13. Chatterjee
14. National Institute of Standards and Technology
15. Forum of Incident Response and Security Teams
16. Base Score
17. Temporal Score
18. Environmental Score
19. Bring Your Own Device
20. Impact sub score
21. Cisco Application Policy Infrastructure Controller