نشریه علمی «پدافند الکترونیکی و سایبری»
سال هشتم، شماره ۲، تابستان ۱۳۹۹؛ ص ۸۱- ۷۵

علمی–پژوهشی

رابطه آسیب‌پذیری نرم‌افزارها و راه‌حل‌های جنبی

عاطفه خزاعی[۱]، محمد قاسم‌زاده[۲*]

۱- دکتری مهندسی نرم‌افزار، ۲- دانشیار گروه مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران

(دریافت: ۹۸/۴/۷، پذیرش: ۹۸/۸/۱)

چکیده

این مقاله به بررسی ارتباط انواع آسیب‌پذیری نرم‌افزارها و راه‌حل‌های جنبی آن‌ها می‌پردازد. یک راه‌حل جنبی روشی است که توسط آن کاربر بدون حذف آسیب‌پذیری، خطر بهره‌کشی ناشی از آن را از بین می‌برد یا کاهش می‌دهد. تاکنون توجه اندکی به این امکانِ بالقوه صورت گرفته است. راه‌حل‌های جنبی می‌توانند در خودکارسازی مقابله با آسیب‌پذیری‌ها بسیار مؤثر باشند. در این پژوهش ابتدا با ترکیب داده‌های حاصل از چهار پایگاه‌داده‌ی مرجعِ آسیب‌پذیری (OSVDB، Security Tracker، Cert CC Vulnerability Notes و NVD)، یک پایگاه‌داده‌ی جدید برای راه‌حل‌های جنبی تدوین گردید. در این پایگاه‌داده که آن را VuWaDB نامیده‌ایم، راه‌حل‌های جنبی در شش دسته‌ی اصلی پیکربندی، اصلاح کد، تغییر مسیر، حذف، دسترسی محدود و ابزارهای کاربردی سازمان‌دهی شده‌اند. تعیین نوع آسیب‌پذیری‌ها مبتنی بر CWEهایی که در NVD به آن‌ها اختصاص داده شده، صورت گرفت. به‌منظور کشف رابطه‌ی آسیب‌پذیری‌ها و راه‌حل‌های جنبی مربوطه، پس از انجام یک بررسی آماری، یک گراف دوبخشی استخراج گردید. نتایج حاصل از این بررسی‌ها در جداول مرتبط ارائه و تحلیل شده‌اند. نتایج حاصله، رابطه آسیب‌پذیری نرم‌افزار و راه‌حل‌های جنبی را در اختیار می‌گذارند.

کلیدواژه‌ها: آسیب‌پذیری نرم‌افزار، راه‌حل جنبی، پایگاه‌داده VuWaDB، CWE، گراف دوبخشی

۱- مقدمه

هرگاه یک آسیب‌پذیری کشف و گزارش می‌شود ارائه‌دهندگان آن محصول در صدد رفع نقیصه مورد نظر برمی‌آیند. اصلاح محصول و ارائه نسخه جدید، غالباً فرآیندی زمان‌بر می‌باشد و در طول این بازه زمانی سامانه‌ها در معرض خطر بهره‌کشی توسط مهاجمان قرار دارند. در چنین شرایطی یکی از مؤثرترین و پرکاربردترین روش‌های مقابله با آسیب‌پذیری‌ها استفاده از راه‌حل‌های جنبی می‌باشد. راه‌حل‌های جنبی، خطر بهره‌کشی از آسیب‌پذیری‌ها را با راه‌کارهایی (همانند تغییر کنترل دسترسی‌ها، فعال‌سازی فیلترها، به‌کارگیری رمز عبور، یا دست‌کاری کد برنامه) کاهش می‌دهند یا از بین می‌برند. به‌عبارت‌دیگر با استفاده از راه‌حل‌های جنبی، کاربران با یک آسیب‌پذیری، بدون از بین بردن آن مقابله می‌کنند [۱-۲].

تا به امروز توجه کافی به جمع‌آوری اطلاعات ساخت‌یافته برای راه‌حل‌های جنبی نشده است. تا آنجا که می‌دانیم هیچ‌یک از پایگاه‌داده‌های آسیب‌پذیری موجود، راه‌حل‌های جنبی را به‌عنوان یک عنصر اطلاعاتی مجزا ثبت نمی‌کنند [۳-۵]. برخی از پایگاه‌داده‌ها، راه‌حل‌های جنبی را برای تعداد اندکی از آسیب‌پذیری‌ها ثبت کرده‌اند. عموماً راه‌حل‌های جنبی ثبت شده در پایگاه‌داده‌های مذکور به‌عنوان بخشی از عنصر راه‌حل در نظر گرفته شده‌اند؛ درحالی‌که فراهم ساختن یک پایگاه‌داده جامع و ساخت‌یافته برای راه‌حل‌های جنبی که مشتمل بر دسته‌بندی‌هایی نیز باشد می‌تواند کمکی شایان به ایجاد سامانه‌های خودکار مقابله با آسیب‌پذیری‌ها بنماید.

هدف این پژوهش پاسخ‌دهی به سؤال زیر می‌باشد: آیا یک ارتباط معنادار میان دسته‌های راه‌حل‌های جنبی و انواع آسیب‌پذیری‌ها وجود دارد؟ برای یافتن پاسخ این سؤال ابتدا مجموعه داده‌هایی مناسب برای راه‌حل‌های جنبی آسیب‌پذیری‌ها گردآوری و پس‌ازآن ارتباط میان دسته‌های راه‌حل‌های جنبی و انواع آسیب‌پذیری‌ها را بررسی می‌کنیم.

در ادامه این مقاله، بخش ۲ به پیشینه پژوهش اختصاص داده شده است. بخش ۳ به چگونگی گردآوری مجموعه داده‌هایی مناسب برای راه‌حل‌های جنبی و انتخاب داده‌هایی مناسب برای انواع آسیب‌پذیری‌ها می‌پردازد. بخش ۴ روش و نتایج تحلیل رابطه را توضیح می‌دهد. در پایان، در بخش ۵ بحث و نتیجه‌گیری در مورد نتایج این پژوهش ارائه می‌شود.

*رایانامه نویسنده پاسخگو: m.ghasemzadeh@yazd.ac.ir

۲- سابقه تحقیق

۲-۱- پژوهش‌های دسته‌بندی آسیب‌پذیری‌ها

اگرچه تعداد گزارش‌های آسیب‌پذیری‌ها بسیار زیاد است، اما علت وقوع و تنوع ساختار در آن‌ها چندان زیاد نیست. یک دسته‌بندی مناسب برای آسیب‌پذیری‌ها، در ساده کردن فهم آن‌ها و ارائه راه‌حل برای آسیب‌پذیری‌ها می‌تواند بسیار مؤثر باشد. تاکنون پژوهش‌های بسیاری در این زمینه انجام شده است، اما به نظر می‌رسد که چالش‌های مختلفی در ارتباط با دسته‌بندی آسیب‌پذیری‌ها وجود دارد که باعث می‌شود همچنان این مسئله مورد توجه پژوهشگران قرار گیرد. به‌طورکلی معیارهای دسته‌بندی آسیب‌پذیری‌ها را می‌توان در موارد زیر خلاصه کرد [۶]:

- دسته‌بندی آسیب‌پذیری‌ها برحسب شیوه بهره‌کشی (مانند [۷-۸])
- دسته‌بندی بر اساس مؤلفه‌های نرم‌افزاری و سخت‌افزاری (مانند [۹])
- دسته‌بندی بر مبنای طبیعت آسیب‌پذیری و دلیل ایجاد آن (مانند [۱۰])
- دسته‌بندی آسیب‌پذیری‌ها با توجه به زمان وقوع آن‌ها (مانند [۱۱])
- دسته‌بندی آسیب‌پذیری‌ها بر مبنای دامنه (مانند [۱۲])

شرکت و همکارانش در مقاله‌ای مروری، پژوهش‌های مرتبط با دسته‌بندی آسیب‌پذیری‌ها را مورد بررسی قرار داده‌اند و به نمونه‌های بیشتری از کارهای انجام شده در این حوزه پژوهشی اشاره کرده‌اند [۶]. اگرچه پژوهش‌های زیادی در این زمینه انجام شده است و هدف بسیاری از این پژوهش‌ها ارائه یک استاندارد برای دسته‌بندی آسیب‌پذیری‌ها بوده است، اما در عمل هیچ‌یک از آن‌ها به این هدف دست نیافته‌اند. در این میان به نظر می‌رسد، CWE [۱۳] توانسته است به این هدف نزدیک‌تر شود.

شرکت غیرانتفاعی آمریکایی MITRE از سال ۱۹۹۹ که شروع به ارائه فهرست CVE کرد، فعالیت خود برای دسته‌بندی آسیب‌پذیری‌ها را نیز آغاز کرد و درنهایت CWE را به‌عنوان معیاری استاندارد برای دسته‌بندی آسیب‌پذیری‌ها ارائه کرد. CWE زبانی متعارف برای کشف، بحث و مقابله با علل آسیب‌پذیری‌های امنیتی نرم‌افزارها که در طراحی، کد یا معماری سامانه یافت شده‌اند، می‌باشد. هر CWE متناظر با یک نوع آسیب‌پذیری می‌باشد. فهرست کامل CWEها و توضیحات آن‌ها در وب‌سایت MITRE موجود است [۱۳]. در این پژوهش از فهرست CWEها برای تعیین نوع آسیب‌پذیری استفاده می‌شود.

۲-۲- پژوهش‌های مرتبط با راه‌حل‌های جنبی

پایگاه‌داده‌های مختلفی برای ثبت و ارائه آسیب‌پذیری‌ها وجود دارد که در پژوهش‌های بسیاری مورد استفاده قرار می‌گیرند. اما در میان این پایگاه‌داده‌ها تعداد کمی از آن‌ها به ثبت راه‌حل‌های جنبی می‌پردازند. تاکنون راه‌حل‌های جنبی به‌عنوان بخشی از عنصر راه‌حل در این پایگاه‌داده‌ها برای تعداد بسیار اندکی از نمونه‌ها ثبت شده است. عملاً تا به امروز توجه کمی به راه‌حل‌های جنبی در پایگاه‌داده‌ها شده است. در این پژوهش برای نخستین بار پایگاه‌داده‌ای (با نام VuWaDB) برای جمع‌آوری، بررسی و ثبت راه‌حل‌های جنبی ارائه شده است. در VuWaDB راه‌حل‌های جنبی دسته‌بندی شده‌اند. هیچ‌یک از پایگاه‌داده‌های آسیب‌پذیری موجود دارای دسته‌بندی برای راه‌حل‌های جنبی نمی‌باشند.

پیش‌ازاین تعداد اندکی از پژوهشگران برای دسته‌بندی راه‌حل‌های آسیب‌پذیری‌ها تلاش‌هایی را انجام داده‌اند، اما هیچ‌یک از آن‌ها همه‌ی انواع آسیب‌پذیری‌ها را مورد بررسی قرار نداده‌اند. برای مثال هووارد در رساله‌ی دکتری خود بر آسیب‌پذیری‌های اینترنت تمرکز کرده است. او دو دسته اصلی برای اقدامات اصلاحی تعریف کرده است: اقدامات داخلی (اقدامات قابل اجرا توسط مدیر سامانه) و اقدامات خارجی (اقدامات قابل اجرا در خارج از سازمان). هر یک از این دسته‌ها مشتمل بر تعدادی زیر دسته می‌باشد [۱۴]. به نظر می‌رسد این پژوهش اولین تلاش به سوی دسته‌بندی اقدامات اصلاحی می‌باشد. البته همان‌طور که پیش‌از این اشاره شد پژوهش یاد شده فقط بر آسیب‌پذیری‌های اینترنت تمرکز داشته است.

پس‌ازآن پژوهشگران دیگری نیز دسته‌بندی‌هایی را برای اقدامات اصلاحی ارائه کردند، اما آن‌ها نیز همانند هووارد به انواع خاصی از آسیب‌پذیری‌ها پرداخته‌اند. برای مثال لی و دیویس بر اقدامات اصلاحی تعدادی از آسیب‌پذیری‌های سامانه‌عامل‌ها تمرکز داشته‌اند [۱۵]. در پژوهشی دیگر، موخو و همکارانش به آسیب‌پذیری‌های هسته لینوکس پرداخته‌اند و با تحلیل کدهای مرتبط، راه‌حل‌هایشان را در ۱۳ گروه دسته‌بندی کرده‌اند [۱۶]. یوآنان [۱۷] و دایک [۱۸] نیز آسیب‌پذیری‌های مرتبط با زبان برنامه‌نویسی C را مطالعه و راه‌حل‌هایشان را دسته‌بندی کرده‌اند.

پژوهشگران فوق علاوه بر این‌که به مطالعه انواع خاصی از آسیب‌پذیری‌ها پرداخته‌اند برای دسته‌بندی راه‌حل‌ها، کدهای نرم‌افزارها را به‌کار گرفته‌اند. این کدها عموماً در دسترس عموم قرار ندارند، بنابراین این تحلیل‌ها و دسته‌بندی‌ها بیش از این‌که برای کاربران مفید واقع گردد برای سازندگان سودمند می‌باشد؛ دسته‌بندی راه‌حل‌های جنبی باید به شکل عمومی‌تر ارائه گردد.

۳- مجموعه داده‌ها

پایگاه‌داده‌های آسیب‌پذیری‌ها به دودسته‌ی اصلی تقسیم می‌شوند: ۱) پایگاه‌داده‌های عمومی، همانند NVD [۱۹] و OSVDB [۲۰]؛ ۲) پایگاه‌داده‌های سازندگان، همانند MFSA [۲۱] و پایگاه‌داده اطلاعات امنیتی لینوکس دبیان [۲۲].

پایگاه‌داده‌های عمومی حاوی گزارش‌های آسیب‌پذیری زیادی در ارتباط با برنامه‌های کاربردی مختلف می‌باشند. درحالی‌که پایگاه‌داده‌های سازندگان اغلب حاوی گزارش‌های آسیب‌پذیری‌های محصولات خاصی می‌باشند؛ بسیاری از این پایگاه‌داده‌ها در دسترس عموم نیستند.

برخی پایگاه‌داده‌های آسیب‌پذیری شامل عنصر اطلاعاتی «راه‌حل» می‌باشند. محتوی این عنصر عموماً جملاتی به زبان طبیعی که نصب یک بسته یا ارتقاء نرم‌افزار را به کاربر توصیه می‌کنند، می‌باشد. در تعداد کمی از این پایگاه‌داده‌ها، راه‌حل‌های جنبی برای تعداد اندکی از آسیب‌پذیری‌ها (در مواردی که بررسی کرده‌ایم به‌طور متوسط برای یک درصد نمونه‌ها) ثبت شده است. بنابراین در این پژوهش برای اینکه بتوانیم تعداد کافی نمونه برای راه‌حل‌های جنبی را جمع‌آوری کنیم، چندین پایگاه‌داده را بررسی و نمونه‌های حاصل از آن‌ها را با هم ادغام کردیم.

برای دست‌یابی به این مقصود پایگاه‌داده‌های OSVDB [۲۰]، Security Tracker [۲۳] و CERT CC Vulnerability Notes [۲۴] برای جمع‌آوری نمونه راه‌حل‌های جنبی بررسی شد. علاوه بر این‌ها، در پایگاه‌داده‌ی NVD [۱۹] برای تعداد اندکی از آسیب‌پذیری‌ها به مراجعی که راه‌حل جنبی را ثبت کرده‌اند نیز اشاره شده است که در این پژوهش آن‌ها را نیز مورد بررسی قرار دادیم. نمونه‌های راه‌حل‌های جنبی جمع‌آوری شده با استفاده از شناسه‌های CVE-ID با یکدیگر ادغام شدند. پایگاه‌داده ارائه شده در این پژوهش (VuWaDB) دارای ۱۲۳۰ نمونه می‌باشد که آسیب‌پذیری‌های متناظر با آن‌ها در بازه زمانی ابتدای سال ۱۹۹۹ تا آوریل ۲۰۱۶ در CVE [۲۵] گزارش شده‌اند. CVE پایگاه‌داده‌ای است که حاوی شناسه‌های استاندارد در نظر گرفته شده برای آسیب‌پذیری‌ها می‌باشد و در دسترس عموم قرار دارد [۲۵]. این نمونه راه‌حل‌های جنبی پس از بررسی بیش از یک‌صدهزار آسیب‌پذیری حاصل شده‌اند. پایگاه‌داده راه‌حل‌های جنبی آسیب‌پذیری‌های خود را VuWaDB نامیده‌ایم.

یکی از دستاوردهای این پژوهش ارائه دسته‌بندی جامع برای راه‌حل‌های جنبی می‌باشد. جدول (۱) دسته‌ها و زیردسته‌های تعریف شده برای راه‌حل‌های جنبی را نشان می‌دهد.

جدول (۱): دسته‌های راه‌حل‌های جنبی در VuWaDB

دسته	زیر دسته	توضیح
پیکربندی	تنظیمات	تغییر دادن تنظیمات
	رمز عبور	تغییر دادن (یا تنظیم کردن) رمز عبور
	فعال‌سازی	فعال‌سازی یک ویژگی
	غیرفعال‌سازی	غیرفعال‌سازی یک ویژگی
اصلاح کد	-	اصلاح کردن کد برنامه
حذف	-	حذف کردن فایل، پوشه، برنامه یا تابع
تغییر مسیر	-	انتقال فایل، پوشه یا تابع به مکانی دیگر
دسترسی محدود	مجوز	تغییر دادن مجوزها
	مسدود کردن	مسدود کردن گذرگاه‌ها
	فیلتر کردن	فیلترکردن بسته‌ها
ابزار کاربردی	-	استفاده کردن از ابزاری کاربردی

شش دسته اصلی برای راه‌حل‌های جنبی تعریف شده است:

۱- پیکربندی: منظور از پیکربندی تنظیم یا تغییر مشخصات اجزای سامانه می‌باشد. زیردسته‌های این دسته عبارت‌اند از: تغییر تنظیمات، تغییر یا تنظیم رمز عبور و فعال یا غیرفعال کردن ویژگی‌های سامانه.

۲- اصلاح کد: با ایجاد تغییر و اصلاح کد برخی نرم‌افزارهای منبع باز می‌توان با بعضی از آسیب‌پذیری‌های آن‌ها مقابله کرد و خطر آن‌ها را کاهش داد یا از بین برد.

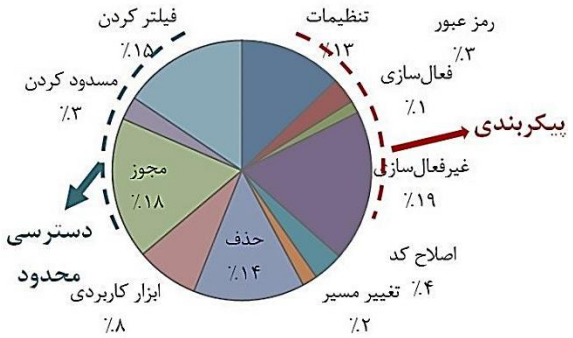
۳- حذف: گاهی با حذف یک فایل، پوشه، برنامه یا تابع بدون نیاز به حذف کامل نرم‌افزار می‌توان خطر یک آسیب‌پذیری را کاهش داد یا از بین برد.

۴- تغییر مسیر: گاهی با تغییر مسیر (منتقل کردن به مکانی دیگر در حافظه) یک فایل، پوشه یا تابع می‌توان خطر یک آسیب‌پذیری را کاهش داد یا از بین برد.

۵- دسترسی محدود: بهره‌کشی از یک آسیب‌پذیری زمانی رخ می‌دهد که مهاجم بتواند به سامانه آسیب‌پذیر دسترسی پیدا کند. بنابراین، در بسیاری از موارد با محدود کردن دسترسی کاربران می‌توان با بهره‌کشی از آسیب‌پذیری‌ها مقابله کرد. این کار را می‌توان با تغییر مجوزها، مسدود کردن برخی گذرگاه‌ها و فیلتر کردن بسته‌ها انجام داد.

۶- ابزار کاربردی: ابزارهای کاربردی نرم‌افزارهایی هستند که با هدف تحلیل، پیکربندی، بهینه‌سازی و نگهداری سامانه‌ها ساخته می‌شوند. برخی از آن‌ها می‌توانند برای بهبود امنیت سامانه‌ها و مقابله با آسیب‌پذیری‌ها استفاده شوند.

پس از جمع‌آوری نمونه‌ها و تعریف دسته‌ها، راه‌حل‌های جنبی ثبت شده در VuWaDB به‌صورت دستی برچسب‌گذاری شدند. جدول (۲) چگونگی توزیع این دسته‌ها را نشان می‌دهد. لازم به ذکر است که راه‌حل‌های جنبی ارائه شده برای برخی از نمونه‌ها (تعداد ۲۰۴ مورد از ۱۲۳۰ نمونه) به بیش از یک دسته تعلق دارند. توزیع دسته‌های راه‌حل‌های جنبی در VuWaDB در شکل (۱) و نشان داده شده اند. در این شکل مشخص است که پیکربندی و دسترسی محدود بزرگ‌ترین دسته‌ها و تغییر مسیر کوچک‌ترین دسته می‌باشند.



شکل (۱): نمایش توزیع دسته‌های راه‌حل‌های جنبی در VuWaDB.

در بخش پیشینه پژوهش به CWE [۱۳] که استاندارد تعریف شده برای انواع آسیب‌پذیری‌ها می‌باشد، اشاره شد. در این پژوهش از CWE برای بررسی روابط میان آسیب‌پذیری‌ها و راه‌حل‌های جنبی آن‌ها استفاده می‌شود.

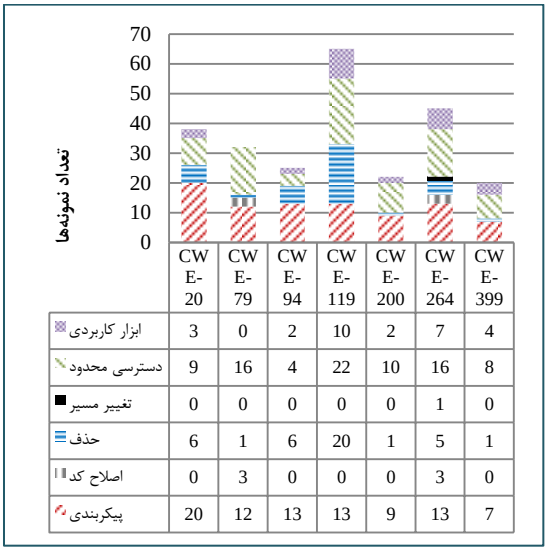
جدول (۲): توزیع دسته‌های راه‌حل‌های جنبی در VuWaDB

دسته	فراوانی دسته	درصد دسته	زیر دسته	فراوانی زیردسته	درصد زیردسته
پیکربندی	۵۳۲	۳۶/۰۰	تنظیمات	۲۰۴	۱۲/۸۷
			رمز عبور	۵۱	۳/۲۲
			فعال‌سازی	۲۴	۱/۵۴
			غیرفعال‌سازی	۲۹۹	۱۸/۸۶
اصلاح کد	۶۰	۴/۰۶	-	۶۰	۳/۷۸
حذف	۱۹۹	۱۳/۴۶	-	۱۹۹	۱۳/۸۸
تغییر مسیر	۳۰	۲/۰۳	-	۳۰	۱/۸۹
دسترسی محدود	۵۳۳	۳۶/۰۶	مجوز	۲۸۰	۱۷/۶۶
			مسدود کردن	۴۶	۲/۹۰
			فیلتر کردن	۲۴۷	۱۵/۵۸
ابزار کاربردی	۱۲۴	۸/۳۹	-	۱۲۴	۷/۸۲

۴- روش و نتایج تحلیل رابطه

هدف این پژوهش بررسی ارتباط میان انواع آسیب‌پذیری‌ها و راه‌حل‌های جنبی آن‌ها می‌باشد. در بخش پیشین پایگاه‌داده VuWaDB معرفی شد. برای بررسی چگونگی این ارتباط، CWEهای متناظر با داده‌های VuWaDB از پایگاه‌داده NVD [۱۹] استخراج شد. در NVD هنوز برای بسیاری از آسیب‌پذیری‌ها CWE ثبت نشده است و فقط توانستیم برای ۴۳۳ مورد از نمونه‌های VuWaDB این اطلاعات را استخراج کنیم.

شکل (۲) توزیع پرتکرارترین CWEها و دسته‌های VuWaDB را برای مجموعه داده‌های نهایی نشان می‌دهد. در این نمودار از انواع کم تکرار CWEها (که دارای فراوانی کمتر از ۲۰ بودند) صرف نظر شده است. همان‌طور که در این نمودار مشخص است CWE-119 متعارف‌ترین نوع آسیب‌پذیری‌ها در VuWaDB می‌باشد. CWE-119 متناظر با آسیب‌پذیری‌های نوع «خطای بافر»می‌باشد.



شکل (۲): توزیع دسته‌های VuWaDB و CWEها.

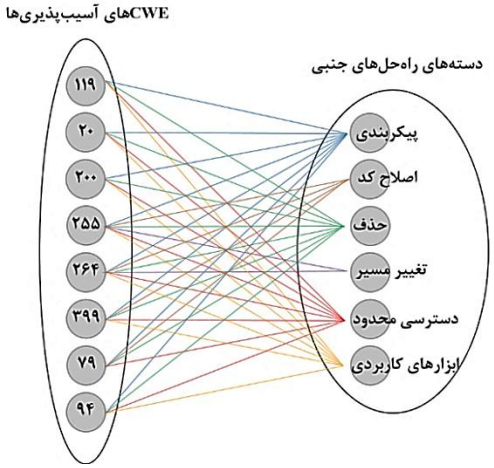
خطای بافر نوعی از آسیب‌پذیری می‌باشد که به مهاجم اجازه تخطی از مرزهای بافر را می‌دهد و منجر به رونویسی در حافظه مجاور می‌گردد.

اطلاعات جدول (۳) را می‌توان در نمایشی ترسیمی به‌صورت یک گراف دوبخشی وزن‌دار نیز ارائه کرد. گره‌های این گراف در یک سو CWEها و در سوی دیگر دسته‌های راه‌حل‌های جنبی هستند. وزن هر یال نیز درصد فراوانی متناظر با آن یال می‌باشد. شکل (۳) این گراف دوبخشی را برای CWEهایی که حداقل دارای ۲۰ نمونه هستند، نمایش می‌دهد. با توجه به فضای محدود موجود برای نمایش گراف، وزن یال‌ها (درصد دسته‌های راه‌حل‌های جنبی در جدول (۳)) نوشته نشده است.

با استفاده از گراف شکل (۳) و جدول (۳) می‌توان دیدی کلی نسبت به نوع راه‌حل‌های جنبی احتمالی برای

آسیب‌پذیری‌های جدید پیدا کرد. برای مثال اگر آسیب‌پذیری جدیدی از نوع CWE-119 (نوع خطای بافر) گزارش شود آنگاه با احتمال ۳۸/۲۰ راه‌حل جنبی از نوع پیکربندی، با احتمال ۳۰/۳۴ راه‌حل جنبی از نوع حذف، با احتمال ۴۱/۵۷ راه‌حل جنبی از نوع دسترسی محدود و با احتمال ۲۲/۴۷ راه‌حل جنبی از نوع ابزار کاربردی را خواهد داشت.

اگر بخواهیم فقط یک نوع از راه‌حل‌های جنبی را به‌عنوان راه‌حل احتمالی این آسیب‌پذیری جدید پیش‌بینی کنیم، راه‌حل جنبی این آسیب‌پذیری با احتمال بیشتر از نوع دسترسی محدود خواهد بود. به‌عبارت‌دیگر می‌توان شکل ساده‌ای از تخمین بیزین را برای پیش‌بینی راه‌حل جنبی برای آسیب‌پذیری‌های جدید به‌کار گرفت.



شکل (۳): گراف دوبخشی رابطه راه‌حل‌های جنبی و CWEها.

جدول (۳): درصد نمونه‌های متعلق به هر دسته راه‌حل‌های جنبی برای CWEهای دارای حداقل ۲۰ نمونه.

CWE--	فراوانی	درصد فراوانی	درصد پیکربندی	درصد اصلاح کد	درصد حذف	درصد تغییر مسیر	درصد دسترسی محدود	درصد ابزار کاربردی
۱۱۹	۸۹	۲۰/۶	۳۸/۲	۰	۳۰/۳	۰	۴۱/۶	۲۲/۵
۲۰	۵۰	۱۱/۶	۵۸	۰	۱۶	۰	۴۰	۱۶
۲۰۰	۳۰	۶/۹	۵۳/۳	۰	۱۳/۳	۰	۴۶/۷	۱۰
۲۵۵	۲۰	۴/۶	۵۰	۵	۵	۱۰	۴۰	۵
۲۶۴	۵۰	۱۱/۶	۲۸	۶	۱۴	۴	۴۲	۱۴
۳۹۹	۳۳	۷/۶	۵۴/۵	۳/۰۳	۲۱/۲	۰	۴۵/۵	۳۰/۳
۷۹	۳۸	۸/۸	۴۲/۱	۷/۸۹	۷/۹	۰	۵۵/۳	۰
۹۴	۲۹	۶/۷	۴۸/۳	۰	۳۱/۰	۰	۲۴/۱	۱۳/۸

با توجه به موارد یاد شده و داده های جدول (۴) ، نتایج زیر بدست می آیند:

- برای همه انواع آسیب‌پذیری‌های مورد بررسی در این پژوهش راه‌حل‌هایی جنبی از دسته‌های پیکربندی، حذف و دسترسی محدود مشاهده شده است.
- راه‌حل‌های جنبی از دسته تغییر مسیر فقط برای آسیب‌پذیری‌های ناشی از ضعف در مدیریت اعتبارنامه‌ها، مجوزها، امتیازات و کنترل‌های دسترسی به‌کاررفته‌اند.
- راه‌حل‌های جنبی از دسته اصلاح کد فقط برای آسیب‌پذیری‌های ناشی از ضعف در مدیریت اعتبارنامه‌ها، مجوزها، امتیازات و کنترل‌های دسترسی، خطاهای مدیریت منابع و XSS به‌کاررفته‌اند.
- ابزارهای کاربردی مقابله با آسیب‌پذیری‌ها فقط در مقابله با آسیب‌پذیری‌های XSS مورد استفاده قرار نگرفته‌اند.

فرضیه این پژوهش این بود که یک ارتباط معنادار میان دسته‌های راه‌حل‌های جنبی و انواع آسیب‌پذیری‌ها وجود دارد. پس از بررسی‌هایی که انجام شد به این نتیجه رسیدیم که این ارتباط چندان قوی و معنادار نمی‌باشد. برای اغلب انواع آسیب‌پذیری‌ها راه‌حل‌های جنبی از تقریباً همه‌ی دسته‌ها موجود است. تعداد نمونه‌های نهایی (نمونه‌هایی که CWE و راه‌حل‌های جنبی برای آن موجود باشد) ۴۳۳ بود که این تعداد نمونه‌ها در مقایسه با کل آسیب‌پذیری‌های گزارش شده کم می‌باشد. بنابراین این نتایج قوی و قابل‌تعمیم به آسیب‌پذیری‌های جدید نمی‌باشند؛ اما برای رد کردن فرضیه کفایت می‌کنند. در این

پژوهش نمونه‌های VuWaDB با بررسی چند پایگاه‌داده‌ی معروف آسیب‌پذیری‌ها گردآوری شدند. تعداد این نمونه‌ها در مقایسه با کل تعداد آسیب‌پذیری‌ها کم می‌باشد. برخی از صفحات وب به راه‌حل‌های جنبی آسیب‌پذیری‌ها اشاره می‌کنند.

جدول (۴): معرفی CWEهای پرتکرار در داده‌های این پژوهش.

CWE	نام	توضیح
CWE-119	خطای حافظه بافر	نرم‌افزار عملیات را در یک حافظه بافر اجرا می‌کند، اما امکان خواندن/نوشتن از/به مکانی از حافظه که خارج از مرزهای تعیین شده‌ی بافر هستند نیز وجود دارد.
CWE-20	تائید اعتبار ورودی نامناسب	نرم‌افزار ورودی‌های ناصحیح را که می‌توانند بر جریان کنترل یا جریان داده تأثیر بگذارند، تائید می‌کند.
CWE-200	افشای اطلاعات	عبارت است از افشای عمدی یا غیرعمدی اطلاعات به شخصی که مجاز به دسترسی به آن اطلاعات نمی‌باشد.
CWE-255	مدیریت اعتبارنامه‌ها	آسیب‌پذیری‌های این دسته مرتبط با ضعف در مدیریت اعتبارنامه‌ها می‌باشد.
CWE-264	مجوزها، امتیازات و کنترل‌های دسترسی	آسیب‌پذیری‌های این دسته مرتبط با مدیریت مجوزها، امتیازات و دیگر مشخصات امنیتی که برای کنترل دسترسی استفاده می‌شوند، می‌باشند.
CWE-399	خطاهای مدیریت منابع	آسیب‌پذیری‌های این دسته مرتبط با مدیریت ناصحیح منابع سامانه می‌باشند.
CWE-79	Cross site Scripting (XSS)	این آسیب‌پذیری‌ها که غالباً در مرورگرهای وب دیده می‌شود باعث می‌شود که داده‌های وارد شده توسط مهاجم به کاربران تحویل داده شود. این داده‌ها می‌توانند کدهای جاوا اسکریپتی باشند که در سمت مرورگر کاربر اجرا می‌شوند.
CWE-94	تزریق کد	این آسیب‌پذیری‌ها منجر به اجرای تمام یا بخشی از یک کد توسط مهاجم بر روی سامانه کاربر می‌شوند.

۵- نتیجه‌گیری

هدف این پژوهش بررسی ارتباط میان نوع آسیب‌پذیری‌های نرم‌افزار و راه‌حل‌های جنبی آن‌ها می‌باشد. ازآنجاکه تاکنون در پایگاه‌داده‌های آسیب‌پذیری‌ها به راه‌حل‌های جنبی آن‌ها توجه کافی نشده است، برای نخستین‌بار به گردآوری و معرفی پایگاه‌داده‌ای برای راه‌حل‌های جنبی پرداختیم. ارائه نخستین پایگاه‌داده راه‌حل‌های جنبی آسیب‌پذیری‌ها و معرفی دسته‌بندی برای آن‌ها از دستاوردهای مهم این پژوهش است.

در ادامه این پژوهش می‌توان برای خودکارسازی گسترش و به‌روزرسانی داده‌های VuWaDB از صفحات وب استفاده کرد. ازآنجاکه نتایج حاصل از این پژوهش قابل‌تعمیم به آسیب‌پذیری‌های جدید نمی‌باشند؛ در پژوهش‌های آتی می‌توان روش‌های یادگیری ماشین را برای پیش‌بینی راه‌حل‌های جنبی برای آسیب‌پذیری‌های جدید به‌کار گرفت.

۶- اقرار و تصدیق

این پژوهش، تحت طرح پژوهشی شماره ۹۴۰۱۲۱۱۳ از سوی «صندوق حمایت از فناوران و پژوهشگران کشور» (INSF) پشتیبانی می‌گردد.

۷- مراجع

[1] H. Holm, "Performance of Automated Network Vulnerability Scanning at Remediating Security Issues," Computers & Security, vol. 31, no. 2, pp. 164-175, 2012.

[2] S. Bejani and M. Abdollahi Azgomi, "Improving the Security of Web Services Based on Intrusion Tolerance Techniques," Journal of Electronical and Cyber Defence, vol. 2, pp. 1-17, 2013. (In Persian)

[3] A. Khazaei and M. Ghasemzadeh, "Software Vulnerability Database Selection Using MoSCoW Prioritization Method," 3rd Int. Conf. on Applied Research in Computer and Information Technology, Tarbiat Modares Uni., Tehran, 2016. (In Persian)

[4] A. Khazaei, M. Ghasemzadeh, and C. Meinel, "VuWaDB: A Vulnerability Workaround Database," Int. Journal of Information Security and Privacy (IJISP), vol. 12, no. 4, pp. 24-34, 2018. (In Persian)

[5] V. Piantadosi, S. Scalabrino, and R. Oliveto, "Fixing of Security Vulnerabilities in Open Source Projects: A Case Study of Apache HTTP Server and Apache Tomcat," 12th IEEE Conference on Software Testing, Validation and Verification (ICST), pp. 68-78, 2019.

[6] M. H. Sherkat, S. Mohammadi, and M. Jamipour, "A Computational Method Based on CVSS For Quantifying the Vulnerabilities in Computer Networks," Iranian Research Institute for Science and Technology, vol. 29, no. 4, pp. 1107-1145, 2014. (In Persian)

[7] A. Kuhnle, N. P. Nguyen, T. N. Dinh, and M. T. Thai, "Vulnerability of Clustering Under Node Failure in Complex Networks," Social Network Analysis and Mining, vol. 7, no. 1, p. 8, 2017.

[8] H. Shahriar and M. Zulkernine, "Taxonomy and Classification of Automatic Monitoring of Program Security Vulnerability Exploitations," Journal of Systems and Software, vol. 84, pp. 250-269, 2011.

[9] J. Ryoo, Y. B. Choi, T. H. Oh, and G. Corbin, "A Multi-Dimensional Classification Framework for Developing Context-Specific Wireless Local Area Network attack Taxonomies," Int. Journal of Mobile Communications, vol. 7, no. 2, pp. 253-267, 2009.

[10] N. V. Juliadotter and K. K. R. Choo, "Cloud Attack and Risk Assessment Taxonomy," IEEE Cloud Computing, vol. 2, no. 1, pp. 14-20, 2015.

[11] H. V. Corcalciuc, "A Taxonomy of Time and State Attacks," Seventh Int. Conference on Availability, Reliability and Security (ARES), pp. 564-573, 2012.

[12] Z. Zhongwen and D. Yingchun, "A New Method of Vulnerability Taxonomy Based on Information Security Attributes," 12th Int. Conf. on Computer and Information Technology, IEEE, pp. 739-741, 2012.

[13] MITRE Corp., "Common Weakness Enumeration (CWE)," http://cwe.mitre.org/, accessed 5 Dec. 2018.

[14] J. D. Howard, "An Analysis of Security Incidents on the Internet 1989-1995," Ph.D. thesis, Carnegie-Mellon University Pittsburgh PA, 1997.

[15] S. C. Lee and L. B. Davis, "Learning From Experience: Operating System Vulnerability Trends," IT professional, vol. 5, no. 1, pp. 17-24, 2003.

[16] S. A. Mokhov, et. al., "Taxonomy of Linux Kernel Vulnerability Solutions," Innovative Techniques in Instruction Technology, Springer Netherlands, pp. 485–493, 2008.

[17] Y. Younan, "An Overview of Common Programming Scurity Vulnerabilities and Possible Solutions," Master Thesis, Vrije Universiteit Brussel, 2003.

[18] V. Dyke, "An In-Depth Analysis of Common Software Vulnerabilities and Their Solutions," Master thesis, Oregon State University, 2004.

[19] NVD, "National Vulnerability Database (NVD)," https://nvd.nist.gov/, accessed 5 Dec 2018.

[20] OSVDB, "Open Source Vulnerability Database," http://osvdb.org/, accessed 5 Dec 2018.

[21] MFSA, "Mozilla Foundation Security Advisories," https://www.mozilla.org/en-US/security/advisories/, Accessed on 5 Dec 2018.

[22] "Debian Linux Security Information," http://www.debian.org, Accessed on 5 Dec. 2018.

[23] "Security Tracker," http://securitytracker.com/, Accessed on 5 Dec. 2018.

[24] "CERT CC Vulnerability Notes Database," https://www.kb.cert.org/vuls/, Accessed on 5 Dec. 2018.

[25] CVE Editorial Board, "Common Vulnerabilities and Exposures," http://cve.mitre.org/, Accessed on 5 Dec. 2018.

Journal of Electronical & Cyber Defence
Vol. 8, No. 2, 2020, Serial No. 30

The relationship of software vulnerabilities and workarounds

A. Khazaei, M. Ghasemzadeh*

*Computer Engineering Group, Yazd University

(Received: 16/12/2018, Accepted: 28/06/2019)

ABSTRACT

This paper investigates the relationship between vulnerability types and their workarounds. Via a workaround solution, users prevent or mitigate the risk of a vulnerability without the need of eliminating it. So far, little attention has been paid to this fruitful approach, whereas workaround solutions can perform so efficiently when dealing with vulnerabilities. In this research, a proper dataset from four mostly referred vulnerability databases (OSVDB, Security Tracker, Cert CC Vulnerability Notes and NVD) is compiled. In this dataset which we have called VuWaDB, the workarounds are organized in six main categories: configuration, code modification, route alteration, elimination, access restriction and utility tools. The CWEs that the NVD was assigned to, are used to determine vulnerability types. In order to discover the relationship between vulnerabilities and their related workaround solutions, after a statistical survey, a relevant bipartite graph is constructed. The obtained results are analyzed and presented in related tables, which provide the relation between software vulnerabilities and their workarounds.

Keywords: Software Vulnerability, Workaround, VuWaDB Database, CWE, Bipartite Graph

* Corresponding Author Email: m.ghasemzadeh@yazd.ac.ir