گزارش بررسی و تحلیل آسیب‌پذیری‌های سیستم‌عامل سرویس‌دهنده‌های مایکروسافت

فهرست مطالب

پیش گفتار

سیستم‌عامل‌ها را می‌توان به عنوان قلب سیستم کامپیوتری تعریف کرد. آن‌ها اولین مولفه نرم‌افزاری هستند که در سیستم بارگذاری می‌شوند و به سیستم امکان اجرا و کنترل را می‌دهند. عملکرد سیستم‌عامل به عنوان مرکز کنترل سیستم نقش آن‌ها را در امنیت کلی سیستم بسیار مهم کرده است. حال اگر این سیستم‌عامل به عنوان بخشی اصلی از سرور استفاده شود و پلتفرم زیرین جهت اجرای سرویس‌های مختلف مانند وب‌سرور و پایگاه‌داده را فراهم آورند، نقش امنیتی آن‌ها بیشتر نیز خواهد شد. این درحالیست که سیستم‌عامل‌ها از هزاران خط کد تشکیل شده‌اند که توسط انسان‌ها طراحی، توسعه شده است. بنابراین امکان وجود صدها آسیب‌پذیری در کد سیستم‌عامل در زمان توسعه سیستم‌عامل ایجاد می‌شود.

در بخشی از رصد و ارزیابی‌های صورت گرفته به صورت حدودی مشخص گردیده‌است که به طور کل ۱۰ نوع سیستم‌عامل مختلف در وبسایت‌های کشور مورد استفاده قرار گرفته است. در بین این سیستم‌عامل‌ها بیشترین سهم با ۸۷٪ متعلق به سرویس‌دهنده های مایکروسافتی می‌باشد. بنابراین تیم تحقیق به بررسی آسیب‌پذیری-های ناشی از استفاده سیستم‌عامل‌های آسیب‌پذیر، پرداخته است. برای این منظور CVEهای منتشر شده برای ویندوز سرورها را تحلیل کرده و لیستی از شدیدترین ضعف‌ها و آسیب‌پذیری‌های ویندوز سرورها را فراهم شده‌است، همچنین لیستی از بروزرسانی‌ها برای آسیب‌پذیری‌ها با شدت بالا تهیه شده است. بعلاوه آسیب-پذیری‌های هر نسخه سیستم‌عامل را به تفکیک مورد تحلیل قرار گرفته‌است.

نتایج کلی

۵۸٪ از آسیب‌پذیری‌های با شدت بالا از طریق شبکه قابل دسترس هستند.

برای ۱۶٪ از آسیب‌پذیری‌های ویندوز سرور کد بهره برداری در سایت های پایگاه آسیب-پذیری‌های مانند exploit-db منتشر شده است.

ویندوز سرور 2012 R2 تحت تاثیر ۵۰٪ از آسیب‌پذیری‌های منتشر شده برای ویندوز می باشد. این ویندوز سرور ۳۷٪ از ویندوز سرورهای شناسایی شده در کشور را تشکیل می دهد.

ویندوز سرور 2008 R2 تحت تاثیر ۷۵٪ از آسیب‌پذیری‌های منتشر شده برای ویندوز می باشد. این ویندوز سرور که ۲۴٪ از ویندوز سرورهای شناسایی شده در کشور را تشکیل می دهد از سال ۲۰۲۰بروزرسانی نخواهد شد.

شدیدترین ضعف ویندوز سرور	شدیدترین آسیب پذیری های ویندوز سرور
مجوزها، امتیازات و کنترل دسترسی	اجرای کد
محدود کردن نادرست عملیات در محدوده یک بافر حافظه	کسب امتیاز
افشای اطلاعات	کسب اطلاعات

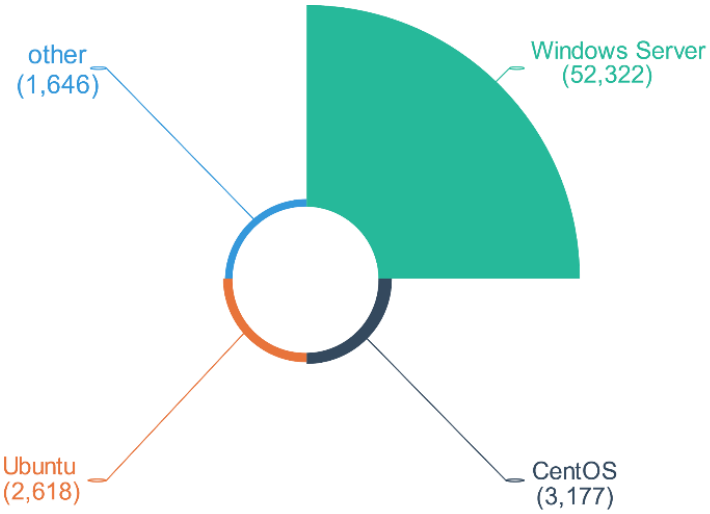
مقدمه

۱-۱- ویندوز سرور

یکی از زیرساخت‌های اصلی در توسعه و راه‌اندازی سیستم‌ها و سامانه‌های تحت وب، سیستم‌عامل می‌باشد که به عنوان پلتفرم زیرین جهت اجرای سرویس‌های مختلف مانند وب‌سرور و پایگاه‌داده مورد استفاده قرار می‌گیرد. سیستم‌عامل‌های لینوکس و ویندوز در طول سالیان دراز برای به‌دست آوردن بازار سیستم‌عامل در چالش بودند. میزان استفاده از هر دو این سیستم‌عامل‌ها در گذر زمان به شدت افزایش یافته است. بر اساس گزارش انواع تکنولوژی‌های ساخت (این گزارش درسال ۱۳۹۷ در اختیار مرکز ماهر قرار گرفته است.) بیش از ۵۵٪ وبسایت‌های بررسی شده اطلاعات مربوط به سیستم‌عامل خود را در سرآیند پاسخ HTTP افشا نمی‌کنند. در مابقی ۴۵٪ وبسایت‌ها که تقریبا شامل ۷۲.۰۰۰ مورد می‌باشد، نوع سیستم‌عامل آن‌ها از طریق پارامترهای سرآیند افشا شده است (با فرض صحیح بودن و عدم مقاوم‌سازی و پیکربندی‌های امنیتی). جدول ۱ انواع سیستم‌عامل‌های شناسایی شده را نمایش می‌دهد. به طور کل ۱۰ نوع سیستم‌عامل مختلف در وبسایت‌های کشور مورد استفاده قرار گرفته است. در بین این سیستم‌عامل‌ها بیشترین سهم با ۸۷٪ متعلق به سرویس‌دهنده‌های مایکروسافت می‌باشد و در رتبه‌های بعدی نیز توزیع‌های مختلف سیستم‌عامل لینوکس و یونیکس، به ویژه CentOS و Ubuntu قرار دارند. با توجه به میزان فراوانی سیستم‌عامل ویندوز، میزان آسیب‌پذیری محصولات مختلف از این سیستم‌عامل را در گذر زمان از جنبه‌های مختلفی مانند تعداد، شدت و نوع آسیب‌پذیری‌ها و ... مورد بررسی قرار گرفته است.

جدول ۱ - انواع سیستم‌عامل‌های شناسایی شده

رتبه	نوع سیستم‌عامل	تعداد
۱	Windows	۵۲.۳۲۲
۲	CentOS	۳.۱۷۷
۳	Ubuntu	۲.۶۱۸
۴	سایر	۱.۶۴۶



شکل ۱-انواع سیستم‌عامل‌های شناسایی شده

CWE -۲-۱

CWE لیستی از انواع ضعف‌های معروف نرم‌افزاری هست که زبان مشترکی را برای بررسی و جست‌وجو آسیب‌پذیری‌های نرم‌افزاری فراهم می‌کند. CWEها به صورت سلسه مراتبی از یک‌دیگر مشتق می‌شوند. شما می‌توانید سلسله مراتب اشتقاق CWEها و پایگاه‌داده تمام CWEها را در سایت Mitre و NIST مشاهده کنید. ۳۲ نوع ضعف، ویندوز سرورها را تحت تاثیر قرار می‌دهد که مهمترین آن‌ها در جدول ۲ نمایش داده شده است. نکته قابل توجه این است که ۸۰٪ از ضعف‌های ویندوز سرورها در ۷ دسته قرار گرفته‌اند.

جدول ۲- انواع ضعف‌های ویندوز سرور

شناسه ضعف	نام ضعف در CWE	توصیف نوع آسیب‌پذیری
CWE-264	مجوزها، امتیازات و کنترل دسترسی	ضعف‌های این دسته‌بندی مرتبط با مدیریت اجازه‌ها، امتیازات و ویژگی‌های امنیتی دیگر هستند که برای کنترل دسترسی استفاده می‌شوند.
CWE-200	افشای اطلاعات	افشای عمدی و غیرعمدی اطلاعات به افرادی که حق دسترسی به آن داده‌ها را ندارند.
CWE-119	محدود کردن نادرست عملیات در محدوده یک بافر حافظه	این ضعف شامل نرم‌افزارهایی است که عملیات را روی بافر حافظه انجام می‌دهد، اما می‌تواند اطلاعاتی را از یک مکان حافظه خارج از مرز مورد مجاز خود در بافر بخواند یا بنویسد.
CWE-20	پردازش نامناسب داده ورودی	این ضعف شامل محصولاتی است که داده‌های خود را به خوبی پردازش نمی‌کنند و این ضعف احتمال تغییر جریان داده یا جریان برنامه را ایجاد می‌کند.

CWE-399	خطای مدیریت منابع	ضعف‌های این دسته‌بندی مرتبط با مدیریت نادرست منابع هستند.
CWE-94	کنترل نادرست تولید کد (تزریق کد)	در این آسیب‌پذیری نرم‌افزار همه یا بخشی از قطعه کد برنامه را بر اساس داده-های ورودی ایجاد می‌نماید. اما المان‌های تاثیرگذار در روند کد به خوبی کنترل نمی‌شوند و این المان‌ها موجب تغییر ساختار یا رفتار برنامه می‌شوند.
CWE-254	7PK - ویژگی امنیتی	در این دسته‌بندی دغدغه اصلی در مورد احراز هویت، کنترل دسترسی، محرمانگی، رمزنگاری و مدیریت امتیازات می‌باشد.
سایر	----	۲۵ نوع آسیب‌پذیری دیگر در ویندوز سرورها دیده شده است که به علت کم بودن تعداد آسیب‌پذیری‌های هر گروه از بررسی آن‌ها صرف نظر شده است.

CVE ۳-۱

برای شناسایی آسیب‌پذیری‌های که ویندوز سرورها را تحت تاثیر قرار می‌دهد از منابع مختلفی استفاده شده است. مهم‌ترین این منابع Common Vulnerability Enumeration (CVE)های منتشر شده توسط MITRE می‌باشد. CVE در واقع شناسنامه منحصر به فردی‌است که به آسیب‌پذیری امنیتی شناسایی شده تخصیص داده می‌شود، به‌عبارتی برای هر آسیب-پذیری امنیتی در حوزه فاوا و صنعتی، شناسنامه‌ای تهیه می‌شود که تمام جزئیات و شرح آسیب‌پذیری و اصلاحیه‌های مربوط به آسیب‌پذیری در CVE اشاره شده است. شرکت NIST برای هر CVE منتشر شده اطلاعات مانند: میزان تاثیر (Impact Ratings) و شدت (Severity Scores) و نحوه رفع آسیب‌پذیری را فراهم می‌کند.

در پایگاه‌داده آسیب‌پذیری‌های NIST از سیستم امتیازدهی آسیب‌پذیری عام Common Vulnerability Scoring System که یک استاندارد آزاد و صنعتی برای ارزیابی و تعیین شدت یک آسیب‌پذیری کامپیوتری می‌باشد، استفاده شده است. این سیستم سعی می‌کند با اختصاص دادن یک امتیاز به میزان شدت آسیب‌پذیری‌ها، به مسئولان و مدیران امنیت سایبری سازمان‌ها این امکان را بدهد تا بتوانند برای رفع آسیب‌پذیری موردنظر اولویت‌بندی کرده و منابع موردنیاز را به آن اختصاص دهند. این امتیازدهی به وسیله فرمولی محاسبه می‌شود که دارای چند معیار است و سعی دارد سهولت بهره‌برداری از آسیب‌پذیری و همچنین اثرات بهره‌برداری آسیب‌پذیری را مشخص کند. امتیازها در بازه ۰ تا ۱۰ قرار دارند، که در آن ۱۰ به شدیدترین تهدید اشاره دارد. در حال حاضر در پایگاه‌داده NIST از دو نسخه CVSSv3.0 و CVSSv2.0 استفاده می-شود. (اما با توجه به اینکه بیشتر CVEها فاقد امتیاز با نسخه CVSSv3.0 می‌باشند، در ادامه این سند شدت تاثیر آسیب-پذیری‌ها بر اساس CVSSv2.0 خواهد بود.)

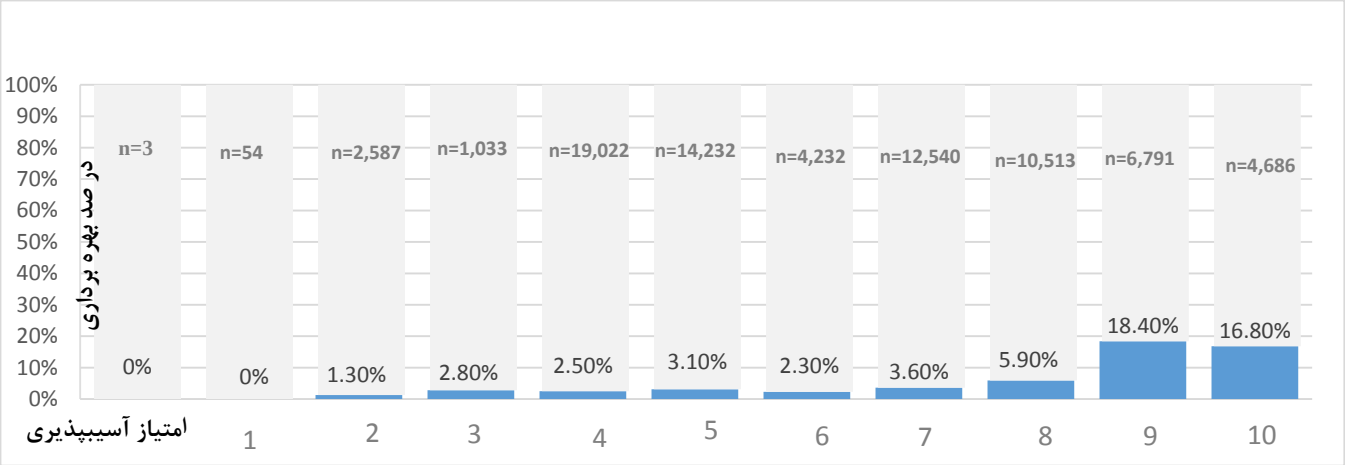
جدول ۳-دامنه امتیاز CVSS v2.0

شدت	رنج امتیاز
کم	۰.۰-۳.۹
متوسط	۴.۰-۶.۹
بالا	۷.۰-۱۰.۰

جدول ۴- دامنه امتیاز CVSS v3.0

شدت	رنج امتیاز
بدون تاثیر	۰.۰
کم	۰.۱-۳.۹
متوسط	۴.۰-۶.۹
بالا	۷.۰-۸.۹
بحرانی	۹.۰-۱۰.۰

محققان با بررسی CVEهای منتشر شده در سال‌های ۲۰۰۸ الی ۲۰۱۸ متوجه شدند که تنها ۵.۵٪ از آسیب‌پذیری‌های منتشر شده در جهان مورد بهره‌برداری عمومی قرار گرفته‌اند. همچنین آن‌ها متوجه شدند که بیشتر آسیب‌پذیری‌های بهره‌برداری شده دارای امتیاز ۹ یا ۱۰ در سیستم امتیازدهی CVSSv2.0 بوده‌اند. نتیجه تحقیقات در شکل ۲ نمایش داده شده است. این محققان، آسیب‌پذیری‌ها را براساس امتیاز دسته‌بندی کردند. تنها سه آسیب‌پذیری با امتیاز ۰ وجود دارد. بیشترین آسیب‌پذیری‌های منتشر شده دارای امتیاز ۴ هستند که شامل ۱۹،۰۲۲ آسیب‌پذیری می‌شود. ۶،۷۹۱ آسیب‌پذیری با امتیاز ۹ وجود دارد که ۱۸.۴۰٪ آنها بهره‌برداری شده‌اند. نکته جالب اینکه ۱۶.۸٪ از آسیب‌پذیری‌ها با امتیاز ۱۰مورد بهره-برداری قرار گرفتند که ۱.۶٪ کمتر از درصد بهره‌برداری آسیب‌پذیری با امتیاز ۹ می‌باشد.



شکل ۲- درصد بهره‌برداری از آسیب‌پذیری‌ها براساس امتیاز آسیب‌پذیری

بررسی CVE منتشر شده نشان می‌دهد که تا مرداد ۱۳۹۸ حدود ۱۸۰۰ آسیب‌پذیری برای ویندوز سرورها منتشر شده است. هر یک از این آسیب‌پذیری‌ها بر اساس نوع آسیب‌پذیری و مولفه آسیب در یک یا چند دسته‌بندی ضعف قرار می‌گیرند. جدول ۵ تعداد آسیب‌پذیری‌های متعلق به هر ضعف را نشان می‌دهد. ضعف مجوزها، امتیازات و کنترل دسترسی در ۴۳۱ آسیب‌پذیری منتشر شده، وجود داشته است و در مرتبه اول ضعف‌های ویندوز سرور قرار دارد و افشای اطلاعات ضعف دوم می‌باشد که در ۳۶۶ آسیب‌پذیری مشاهده شده است. توجه به این نکته ضروریست که رابطه بین ضعف و آسیب‌پذیری رابطه علت و معلول می‌باشد. این به این معناست که وجود ضعف در سیستم موجب بروز آسیب‌پذیری می‌شود.

جدول ۵- دسته‌بندی آسیب‌پذیری‌ها بر اساس ضعف

رتبه	شناسه ضعف	تعداد آسیب پذیری
۱	مجوزها، امتیازات و کنترل دسترسی	۴۳۱
۲	افشای اطلاعات	۳۶۶
۳	محدود کردن نادرست عملیات در محدوده یک بافر حافظه	۲۲۶
۴	پردازش نامناسب داده ورودی	۲۱۰
۵	خطای مدیریت منابع	۸۹
۶	کنترل نادرست تولید کد (تزریق کد)	۸۴
۷	7PK - ویژگی امنیتی	۶۵
۸	سایر	۳۲۳

۱-۴- انواع آسیب‌پذیری‌ها

منابع مختلفی اقدام به بررسی جزئیات آسیب‌پذیری‌های منتشر شده می‌کنند. یکی از این منابع، سایت www.cvedetails.com می‌باشد. در این سایت برای هر CVE نوع آسیب‌پذیری مشخص می‌شود. براساس بررسی‌های انجام شده، ۱۰ نوع آسیب‌پذیری در ویندوز سرورها وجود دارد. هر CVE ممکن است در یک یا چند دسته از انواع آسیب‌پذیری‌ها قرار بگیرند. جدول ۶ تعداد CVEهای هر نوع آسیب‌پذیری ویندوز سرور را نشان می‌دهد.

جدول ۶- انواع آسیب‌پذیری ویندوز سرورها

ردیف	نام	معادل فارسی	تعداد آسیب‌پذیری
۱	Execute Code	اجرای کد	۴۳۱
۲	Gain privileges	کسب امتیاز	۳۶۶
۳	Obtain Information	کسب اطلاعات	۲۲۶
۴	Overflow	سرریز	۲۱۰
۵	Denial Of Service	انکار سرویس	۸۹
۶	Bypass a restriction or similar	دور زدن محدودیت	۸۴
۷	Memory corruption	تخریب حافظه	۶۵
۸	Cross Site Scripting	XSS	۹
۹	Directory traversal	پیمایش مسیر	۲
۱۰	Cross-Site Request Forgery	CSRF	۱

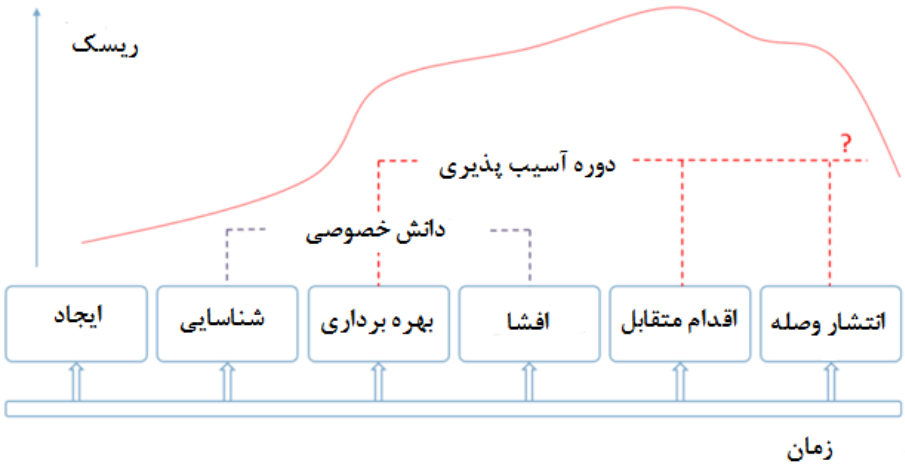
همانطور که قبلا نیز بیان شد ضعف‌ها خطاهای نرم‌افزاری هستند که موجب بروز آسیب‌پذیری‌ها می‌شوند. در واقع CWE یا همان ضعف دسته‌بندی مختلفی است که برای این ضعف‌ها قائل هستیم. یک ضعف مشخص در سیستم ممکن است در آسیب‌پذیری‌های مختلف مورد سوءاستفاده قرار بگیرد. در واقع یک آسیب‌پذیری ممکن است علت چند آسیب‌پذیری باشد. خود این آسیب‌پذیری‌ها بر اساس نحوه بهره‌برداری و امتیازاتی که بعد از بهره‌برداری کسب می‌کنند دسته‌بندی شده و انواع آسیب‌پذیری‌ها را تشکیل می‌دهند.

۱-۵- آسیب‌پذیری در گذر زمان

رخدادهای مختلفی برای یک آسیب‌پذیری در طول زمان اتفاق می‌افتد. شکل ۳ مجموعه این رخدادها را نشان می‌دهد. یک آسیب‌پذیری از زمان ایجاد توسط توسعه‌دهندگان تا زمان که توسط محققان یا هکرها شناسایی شود، ناشناخته می‌باشد. (البته اگر در زمان ایجاد، توسعه‌دهندگان آسیب‌پذیری را به صورت تعمدی و به عنوان در پشتی قرار نداده باشند.)

آسیب‌پذیری می‌تواند توسط اشخاص مختلفی شناسایی شود. بر اساس اینکه چه کسی آسیب‌پذیری را شناسایی کرده باشد، رخدادهای مختلفی ممکن است اتفاق بیافتد. برای مثال ممکن است یک نفوذگر سال‌ها از یک آسیب‌پذیری بهره‌برداری کرده و هیچ اطلاعاتی افشا نکند. اما اگر آسیب‌پذیری توسط مسئول امنیت سیستم یا هکرهای کلاه سفید شناسایی شود؛ در این صورت برای مدتی (حدود یک ماه یا بیشتر) به مالک سیستم زمان داده می‌شود تا آسیب‌پذیری را رفع کند و بعد از این

مدت آسیب‌پذیری به صورت عمومی منتشر شده و شناسه CVE دریافت می‌کند. اما در دنیای واقعی هم هکرها و هم محققان امنیتی به صورت موازی در حال بررسی محصولات مختلف هستند و تمام این رخدادها می‌توانند با هم در حال وقوع باشد. نکته قابل توجه این است که اولا برای امنیت سیستم باید حداقل از زمان عمومی شدن یک آسیب‌پذیری تا زمان ارائه وصله، هر سازمانی بتواند با راهکارهای جایگزین امنیت سامانه‌های خود را تامین کند و نکته مهم‌تر اینکه باید هر سازمان به محض ارائه وصله آسیب‌پذیری سامانه خود را رفع نماید. بررسی محققان نشان می‌دهد که حتی بعد از ارائه وصله برای آسیب‌پذیری‌ها همچنان برخی از سیستم‌ها به دلایل مختلف آسیب‌پذیر باقی می‌مانند. سوال مهم این است که آیا ویندوز سرور شما امن است؟ با آخرین آسیب‌پذیری‌های منتشر شده برای آن آشنا هستید؟ چه نوع ضعف‌هایی بیشتر ویندوز سرور شما را تهدید می‌کنند؟



شکل ۳- آسیب‌پذیری در گذر زمان

۱-۶- بروزرسانی و وصله‌های ویندوز سرور

امنیت سیستم‌عامل سرویس‌دهنده‌های مایکروسافتی مانند دیگر موارد مشابه صد در صد نیست و احتمال وجود رخنه امنیتی، خطا و مولفه‌های قدیمی در آن‌ها وجود دارد. وصله‌های امنیتی، آسیب‌پذیری و خطاهای موجود در ویندوز و نرم-افزارهای مرتبط با آن را رفع می‌کنند و ویژگی‌های جدید به ویندوز سرور اضافه می‌کنند. در واقع به سه دلیل زیر باید همواره ویندوز سرور خود را بروزرسانی می‌گردد.

- حفاظت از سیستم خود در برابر نرم‌افزارهای مخرب و باج‌افزارها
- رفع مشکلات و باگ‌های ویندوز
- دسترسی به ویژگی‌های جدید در ویندوز سرور

مایکروسافت وصله‌هایش را با روش‌های مختلفی منتشر می‌کند. در واقع از اکتبر سال ۲۰۱۶ روش انتشار وصله‌های مایکروسافت تغییر کرده است به این صورت که چندین وصله را با هم در یک بروزرسانی قرار می‌دهد و این روش را بروزرسانی Rollup می‌خواند و Rollupهای ماهانه دارای وصله‌های قبلا منتشر شده نیز هستند و کاربر فقط نیازمند نصب آخرین وصله می‌باشد. در ضمیمه ۱ لیست وصله‌های منتشر شده برای آسیب‌پذیری‌های با شدت بالا مشخص شده است. برای هر آسیب‌پذیری ممکن است چند لینک بروزرسانی وجود داشته باشد که در واقع به وصله محصولات مختلف اشاره دارد. اکثر بروزرسانی‌ها از نوع Security update یا Security-only update هستند. هر دو نوع بروزرسانی برای محصولات مختلف ممکن است ارائه شود، با این تفاوت که Security-only شامل تمام Security updateهای منتشر شده برای یک محصول در یک ماه می‌باشد.

براساس بررسی‌های انجام شده، ۹۵۰ آسیب‌پذیری با شدت بالا ویندوز سرورها را تحت تاثیر قرار می‌دهد که مایکروسافت برای ۹۳۸ مورد وصله ارائه کرده و تنها برای ۱۲ آسیب‌پذیری که در ضمیمه ۱ با رنگ قرمز مشخص شدند راه حلی ارائه نشده است. نکته جالب اینکه کد بهره‌برداری سه مورد از آسیب‌پذیری با شناسه CVE-2009-3020، CVE-2017-8487، CVE-2010-2549 را می‌توان در سایت‌های از جمله Exploit-db مشاهده کرد. برای دسترسی به بروزرسانی آسیب‌پذیری-ها، در صورتی که وصله برای قبل از سال ۲۰۱۶ باشد از آدرس https://docs.microsoft.com استفاده کنید ولی در صورتی که وصله در سال‌های اخیر منتشر شده باشد، شماره ارجاع وصله را در سایت https://support.microsoft.com جست‌وجو کنید.

۱-۷- شیوه جمع‌آوری اطلاعات

داده‌های استفاده شده در این گزارش از منابع مختلفی جمع‌آوری شدند. یکی از مهم‌ترین این منابع داده مرتبط با میزان استفاده از ویندوز سرورها در کشور می‌باشد که توسط خزشگر فضای وب کشور تامین شد. منبع دیگر پایگاه‌داده آسیب‌پذیری‌های NIST می‌باشد. این پایگاه‌داده در زمان نگارش این مقاله دارای ۱۲۷۰۰۰ رکورد بوده است.

پس از جمع‌آوری کل CVEها، آسیب‌پذیری‌هایی که ویندوز سرور را تحت تاثیر قرار می‌دهند، شناسایی شدند. برای این منظور تمام آسیب‌پذیری‌های شرکت مایکروسافت بررسی شدند. سپس آسیب‌پذیری‌هایی که نسخه‌های مختلف ویندوز سرورها را تحت تاثیر قرار می‌دادند، جدا شدند. در واقع در ادامه سند همواره این آسیب‌پذیری‌ها که حدودا شامل ۱۸۰۰ رکورد می‌باشند بررسی می‌شوند.

در ادامه برای کسب اطلاعاتی مانند تعداد کدهای بهره‌برداری شده، وصله‌های منتشر شده برای آسیب‌پذیری‌ها و انواع آسیب‌پذیری‌ها به ترتیب سه سایت Exploit-db و Microsoft و Cvedetails توسط خزشگر فضای وب جست‌وجو شده اطلاعات مورد نظر جمع‌آوری شد.

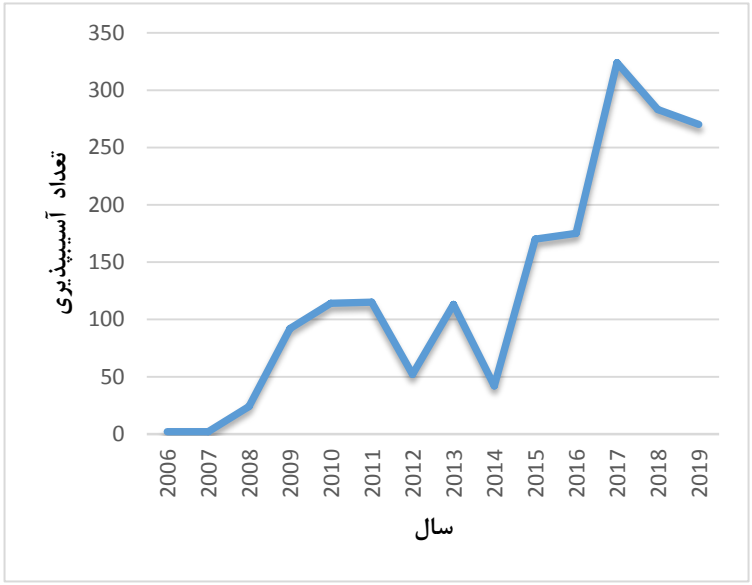
بررسی آسیب‌پذیری ویندوز سرورها

۲-۱ فراوانی آسیب‌پذیری ویندوز سرور

با وجود اینکه CVEها ازسال ۱۹۹۹ ارائه شدند؛ اما بر اساس بررسی‌های ما اولین CVE ارائه شده برای ویندوز سرورها متعلق به سال ۲۰۰۶ می‌باشد. تعداد آسیب‌پذیری‌های منتشر شده برای ویندوز سرورها در گذر زمان صرف نظر از سال‌های ۲۰۱۲ و ۲۰۱۴ و ۲۰۱۸ به صورت مداوم و با شدت زیادی در حال افزایش بوده است. تعداد آسیب‌پذیری‌ها در سال ۲۰۰۶ با ۲ آسیب‌پذیری منتشر شده در کمترین میزان خود قرار داشته و بیشترین میزان آسیب‌پذیری‌های منتشر شده تا به امروز در سال ۲۰۱۷ با ۳۲۴ تعداد آسیب‌پذیری بوده است.

جدول ۷– فراوانی آسیب‌پذیری ویندوز سرورها در سال‌های مختلف

سال	تعداد آسیب‌پذیری‌ها
۲۰۰۶	۲
۲۰۰۷	۲
۲۰۰۸	۲۴
۲۰۰۹	۹۲
۲۰۱۰	۱۱۴
۲۰۱۱	۱۱۵
۲۰۱۲	۵۲
۲۰۱۳	۱۱۳
۲۰۱۴	۴۲
۲۰۱۵	۱۷۰
۲۰۱۶	۱۷۵
۲۰۱۷	۳۲۴
۲۰۱۸	۲۸۳
۲۰۱۹	۲۷۰



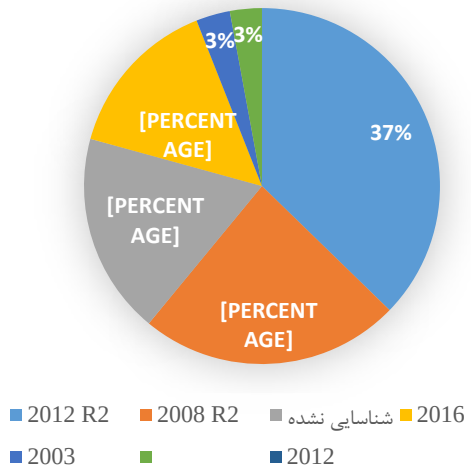
شکل ۴- نمودار فراوانی آسیب‌پذیری ویندوز سرورها در سال‌های مختلف

همان طور که قبلا نیز اشاره گردید، آسیب‌پذیری با شناسه مشخص می‌تواند در بیش از یک محصول تاثیر بگذارد و حتی نسخه‌های مختلف یک محصول را تحت تاثیر قرار دهد. بنابرین نباید از تعداد زیاد آسیب‌پذیری‌های هر ویندوز سرور تعجب

کنیم. در واقع ۸۰۰،۱ CVE منتشر شده برای ویندوز سرورها، ۳،۸۹۲ نسخه مختلف از محصولات مایکروسافت را تحت تاثیر قرار داده است. میزان آسیب‌پذیری محصولات و حتی نسخه‌های مختلف یک محصول متفاوت است. برای بررسی و آگاهی از میزان تهدید منابع کشور ابتدا محصولات مختلف ویندوز سرورها که در وبسایت‌های سطح کشور مورد استفاده قرار گرفته است، مطالعه شد. جدول ۸ فراوانی نسخه‌های مختلف ویندوز سرور را نشان می‌دهد. بر اساس نتایج بررسی‌ها و تحقیقات انجام شده، ویندوز سرور نسخه 2012 R2 و2008 R2 به ترتیب بیشترین میزان استفاده را داشته‌اند و سایر نسخه‌های آن نیز در رتبه‌های بعدی قرار دارند.

رتبه	محصول	نسخه	تعداد
۱	ویندوز سرور ۲۰۱۲	R2	۱۹.۴۰۶
		-	۱.۵۱۱
۲	ویندوز سرور ۲۰۰۸	R2	۱۲.۳۳۸
۳	ویندوز سرور	شناسایی نشده	۹.۵۳۰
۴	ویندوز سرور ۲۰۱۶	-	۷.۶۷۲
۵	ویندوز سرور ۲۰۰۳	-	۱.۶۰۹

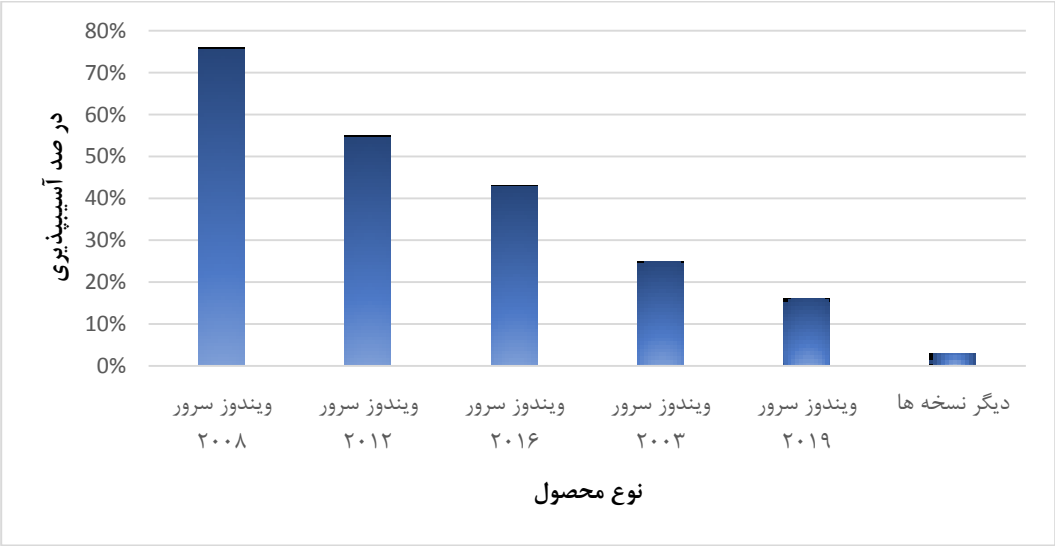
جدول ۸- فراوانی نسخه‌های مختلف ویندوز سرور



شکل ۵- میزان استفاده از نسخه‌های مختلف ویندوز سرور

در شکل ۶ میزان تاثیر آسیب‌پذیری‌های منتشر شده بر روی محصولات و نسخه‌های مختلف ویندوز سرور نمایش داده شده است. ویندوز سرور ۲۰۱۲ و ۲۰۰۸ علاوه بر نسخه معمول نسخه‌های دیگری نیز دارند که معروف‌ترین این نسخه‌ها ویندوز سرور 2008 R2 و 2012 R2 می‌باشند. ویندوز سرور ۲۰۰۸ تحت تاثیر ۷۵٪ از آسیب‌پذیری‌های منتشر شده برای ویندوز سرورها می‌باشد. ۹۸٪ از آسیب‌پذیری‌های منتشر شده برای این محصول، نسخه‌ی 2008 R2 را نیز تحت تاثیر قرار می‌دهند.

بررسی‌های ما نشان می‌دهد که بیش از ۱۹۰۰۰ سایت دارای ویندوز سرور 2012 R2 ، تحت تاثیر نیمی از آسیب‌پذیری‌های منتشر شده برای ویندوز سرورها می‌باشند. ۹۴٪ از آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۱۲ نسخه 2012 R2 را نیز تحت تاثیر قرار می‌دهد. نکته قابل توجه این است که فقط ۵۵ آسیب‌پذیری برای دیگر محصولات ویندوز سرور منتشر شده است. که این مهم نشان دهنده اهمیت نسخه‌های بررسی شده در این سند می‌باشد.

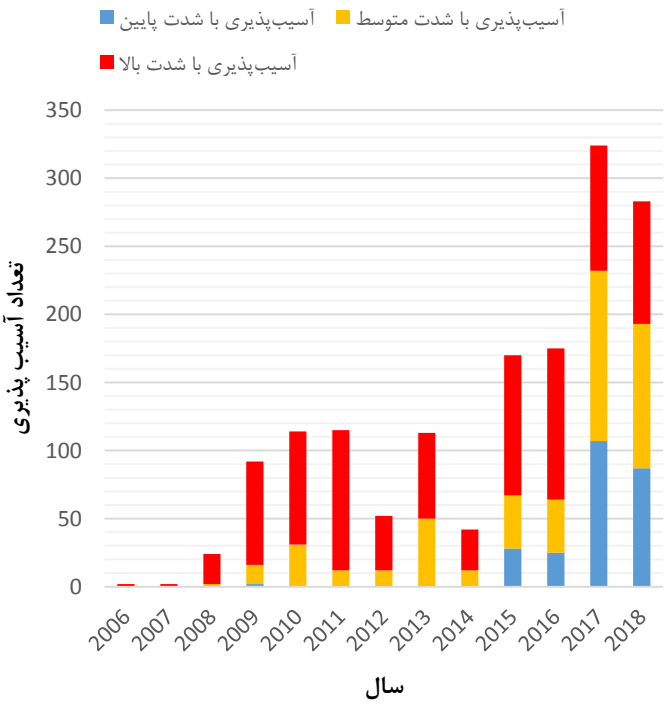


شکل ۶- میزان آسیب‌پذیری محصولات مختلف ویندوز سرور

بر اساس ارزیابی‌های انجام شده، ۵۴٪ از آسیب‌پذیری‌های منتشر شده برای ویندوز سرورها دارای شدت بالا هستند و بیش از نیمی از آن‌ها در ۵ سال اخیر منتشر شده‌اند. در مقابل، آسیب‌پذیری‌ها با شدت پایین تنها ۱۶٪ از کل آسیب‌پذیری‌ها را تشکیل می‌دهند و تقریبا همه آن‌ها در ۵ سال اخیر گزارش شده است. بنابراین علاوه بر افزایش تعداد آسیب‌پذیری باشدت بالا در سال‌های اخیر، تعداد آسیب‌پذیری‌ها با شدت پایین و متوسط نیز به شدت افزایش یافته است. دلیل این اتفاق اولا افزایش تعداد محصولات ثانیا افزایش تمایل به بیان عمومی آسیب‌پذیری‌ها و اجبار مالکان محصول برای پاسخ‌گویی به این ضعف‌ها و رفع آن‌ها می‌باشد. جدول ۹ شدت آسیب‌پذیری منتشر شده برای ویندوز سرور را در طول سال‌های ۲۰۰۶ تا ۲۰۱۹ نمایش داده است.

جدول ۹- شدت آسیب‌پذیری منتشر شده برای ویندوز سرور

سال	شدت آسیب‌پذیری		
	پایین	متوسط	بالا
۲۰۰۶	۲	۰	۰
۲۰۰۷	۲	۰	۰
۲۰۰۸	۲۲	۲	۰
۲۰۰۹	۷۶	۱۴	۲
۲۰۱۰	۸۳	۳۱	۰
۲۰۱۱	۱۰۳	۱۱	۱
۲۰۱۲	۴۰	۱۱	۱
۲۰۱۳	۶۳	۴۹	۱
۲۰۱۴	۳۰	۱۲	۰
۲۰۱۵	۱۰۳	۳۹	۲۸
۲۰۱۶	۱۱۱	۳۹	۲۵
۲۰۱۷	۹۲	۱۲۵	۱۰۷
۲۰۱۸	۹۰	۱۰۶	۸۷
۲۰۱۹	۱۳۳	۹۹	۳۸



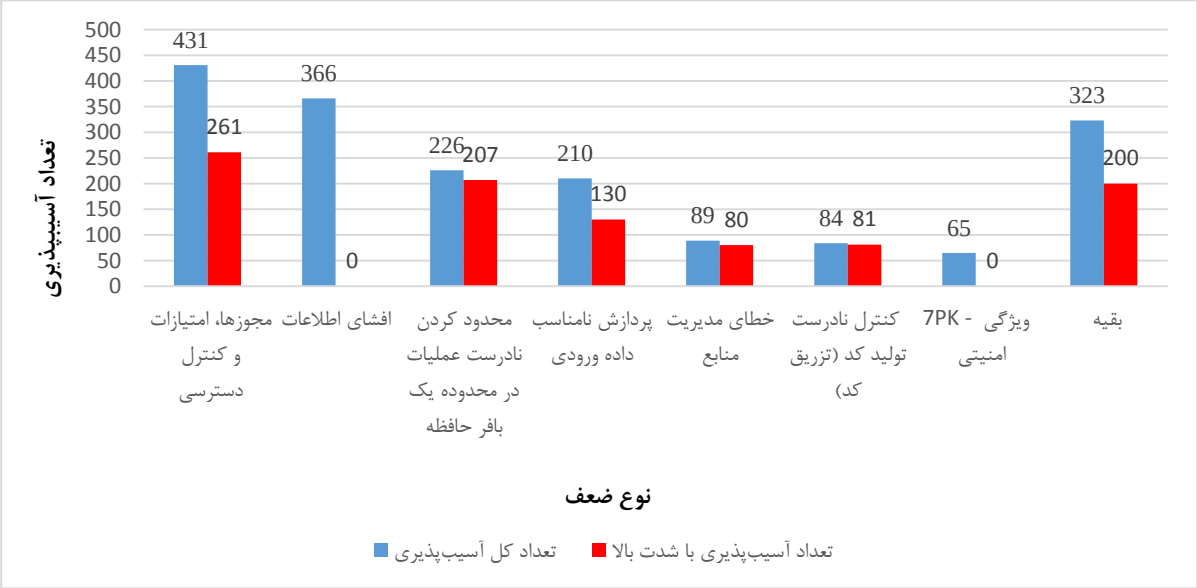
شکل ۷- نمودار شدت آسیب‌پذیری منتشر شده برای ویندوز سرور

۲-۲- بررسی ضعف‌های ویندوز سرورها

در جدول۱۰ مقایسه کمی آسیب‌پذیری‌های ویندوز سرور و آسیب‌پذیری‌های با شدت بالای این سیستم‌عامل بر اساس میزان ضعف مقایسه شده است. بیشترین تعداد آسیب‌پذیری منتشر شده برای ویندوز سرورها با ۴۳۱ عدد از نوع ضعف مجوزها، امتیازات و کنترل دسترسی می‌باشند و بعد از آن افشای اطلاعات با ۳۶۶ آسیب‌پذیری در رتبه دوم انواع ضعف‌ها قرار دارد. با بررسی نمودار ضعف ویندوز سرورها بر اساس آسیب‌پذیری با شدت بالا متوجه خواهیم شد که با وجود اینکه ۲۰٪ از ضعف‌ها را افشای اطلاعات تشکیل می‌دهد ولی این ضعف موجب بروز آسیب‌پذیری با شدت بالا نشده است. این در حالیست که تعداد آسیب‌پذیری‌های از نوع ضعف "محدود کردن نادرست عملیات در محدوده بافر حافظه" با در نظر گرفتن شرط انتخاب آسیب‌پذیری‌ها باشدت بالا و بدون در نظر گرفتن این شرط تقریبا برابر است که این مهم از اهمیت این نوع ضعف در ویندوز سرورها خبر می‌دهد.

جدول ۱۰- مقایسه تعداد کل آسیب‌پذیری‌ها با تعداد آسیب‌پذیری با شدت بالا بر اساس نوع ضعف

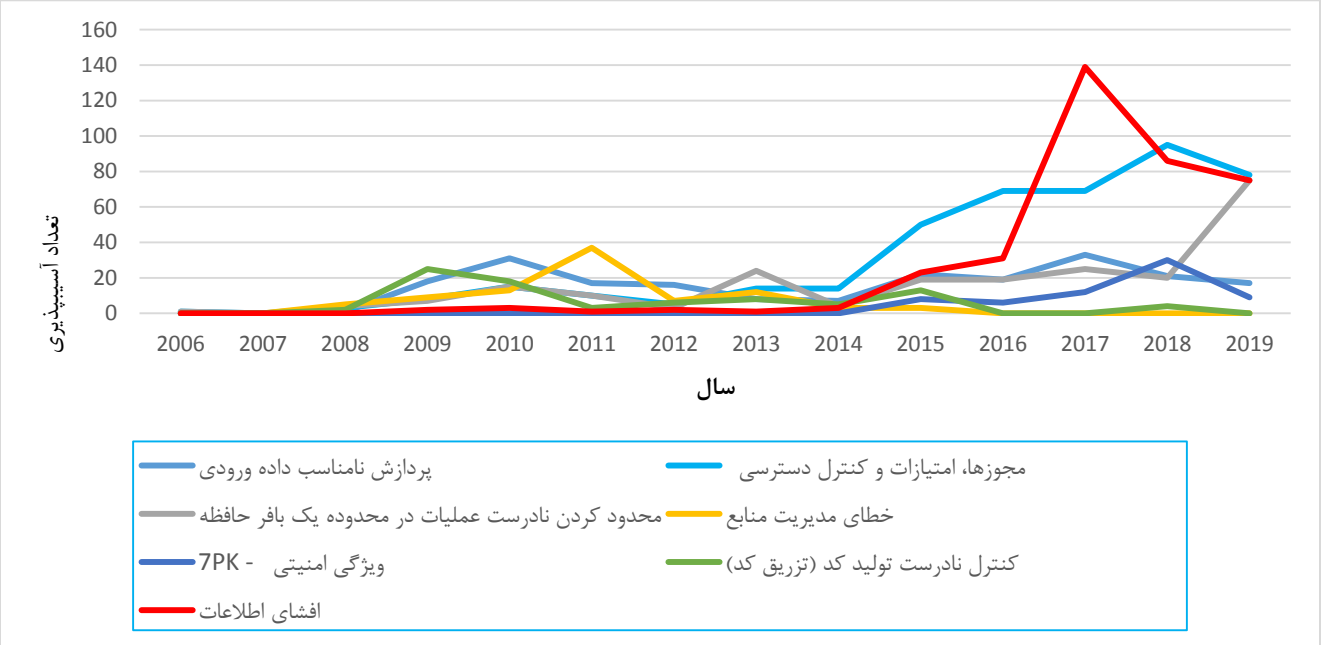
نوع ضعف	تعداد آسیب‌پذیری	آسیب‌پذیری با شدت بالا	آسیب‌پذیری با شدت بالا / تعداد آسیب‌پذیری
مجوزها، امتیازات و کنترل دسترسی	۴۳۱	۲۶۱	٪۶۰
افشای اطلاعات	۳۶۶	۱	٪۲۷
محدود کردن نادرست عملیات در محدوده یک بافر حافظه	۲۲۶	۲۰۷	٪۹۲
پردازش نامناسب داده ورودی	۲۱۰	۱۳۰	٪۶۲
خطای مدیریت منابع	۸۹	۸۰	٪۹۰
کنترل نادرست تولید کد (تزریق کد)	۸۴	۸۱	٪۹۶
PK۷ - ویژگی امنیتی	۶۵	۷	۱۱٪
دیگر موارد	۳۲۳	۱۹۲	٪۵۹



شکل ۸- مقایسه تعداد کل آسیب‌پذیری‌ها با تعداد آسیب‌پذیری با شدت بالا بر اساس نوع ضعف

شکل ۹ نشان می‌دهد که نوع ضعف ویندوز سرورها چگونه در طول سال‌ها تغییر کرده است. به صورت کلی افزایش تعداد CVE باعث شده تا تعداد CVEهای متعلق به هر نوع ضعف نیز در گذر زمان افزایش یابد و برخی از انواع ضعف‌ها مانند پردازش نامناسب داده‌های ورودی، افشای اطلاعات، 7PK-ویژگی امنیتی که در سال‌های اولیه وجود نداشت در گذر زمان

ویندوز سرورها را تحت تاثیر قرار داده است. کاهش تعداد آسیب‌پذیری‌ها در سال‌های ۲۰۱۲ و ۲۰۱۴ به صورت مشهود در نمودارهای تغییر روند نوع ضعف‌ها نیز قابل مشاهده است. بطوریکه بسیاری از ضعف‌ها در این دو سال به کمترین میزان خود رسیدند. پس از کاهش نسبی همه ضعف‌ها در سال ۲۰۱۴، افزایش قابل ملاحظه‌ای در انواع مختلف ضعف‌ها رخ داده است. ضعف افشای اطلاعات از جمله ضعف‌هایی است که بعد از سال ۲۰۱۴ جهش قابل ملاحظه‌ای داشته و در سال ۲۰۱۷ به اوج رسیده و پس از آن رو به کاهش گذاشته است. با وجود اینکه در اواسط سال ۲۰۱۹ می‌باشیم؛ افزایش نسبی در انواع ضعف‌ها مانند ضعف تولید نامناسب ایجاد کد قابل مشاهده است.



شکل ۹- روند تغییر نوع ضعف ویندوز سرور

جدول ۱۱- روند تغییر نوع ضعف ویندوز سرور در طول سال‌ها

سال	پردازش نامناسب داده ورودی	مجوزها، امتیازات و کنترل دسترسی	محدود کردن نادرست عملیات	خطای مدیریت منابع	ویژگی7PK امنیتی	کنترل نادرست تولید کد کد	افشای اطلاعات
۲۰۰۶	۰	۱	۱	۰	۰	۰	۰
۲۰۰۷	۰	۰	۰	۰	۰	۰	۰
۲۰۰۸	۱	۳	۴	۵	۰	۲	۰
۲۰۰۹	۱۸	۸	۷	۹	۰	۲۵	۲
۲۰۱۰	۳۱	۱۵	۱۵	۱۳	۰	۱۸	۳
۲۰۱۱	۱۷	۱۰	۱۰	۳۷	۰	۳	۱
۲۰۱۲	۱۶	۵	۳	۷	۰	۶	۲
۲۰۱۳	۸	۱۴	۲۴	۱۲	۰	۸	۱
۲۰۱۴	۷	۱۴	۴	۳	۰	۵	۳
۲۰۱۵	۲۲	۵۰	۱۹	۳	۸	۱۳	۲۳
۲۰۱۶	۱۹	۶۹	۱۹	۰	۶	۰	۳۱
۲۰۱۷	۳۳	۶۹	۲۵	۰	۱۲	۰	۱۳۹
۲۰۱۸	۲۱	۹۵	۲۰	۰	۳۰	۴	۸۶
۲۰۱۹	۱۷	۷۸	۷۵	۰	۹	۰	۷۵

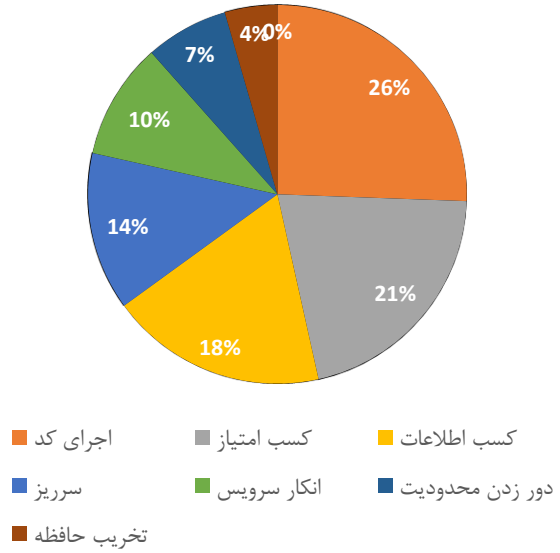
۲-۳- بررسی انواع آسیب‌پذیری ویندوز سرورها

در شکل۱۰ مشاهده می‌شود که ۲۵٪ از کل انواع آسیب‌پذیری‌ها را در ویندوز سرورها آسیب‌پذیری اجرای کد تشکیل می-دهد. کسب امتیاز با ۲۱٪ در رتبه دوم قرار دارد. حال با توجه به اهمیت آسیب‌پذیری با شدت بالا اگر انواع آسیب‌پذیری‌ها را فقط برای آسیب‌پذیری‌ها با شدت بالا (شکل ۱۱) بررسی‌کنیم. با توجه به افزایش درصد دو نوع آسیب‌پذیری اجرای کد و کسب امتیاز متوجه می‌شویم که بسیاری از آسیب‌پذیری‌های این دو دسته‌بندی دارای شدت بالا هستند. همچنین نوع

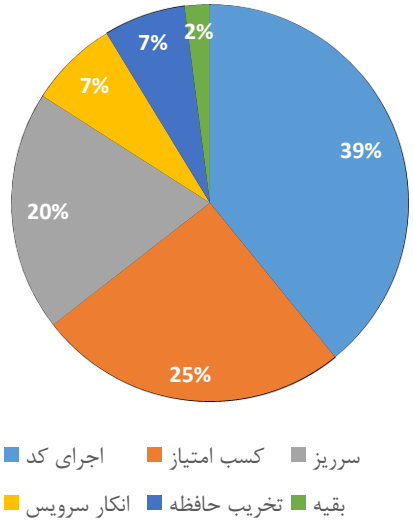
آسیب‌پذیری کسب اطلاعات و دور زدن محدودیت ارزش خود را از دست می‌دهند و این نوع آسیب‌پذیری‌ها در ویندوز سرور دارای شدت بالا نیستند.

جدول ۱۲- انواع آسیب‌پذیری‌های ویندوز سرور

نوع آسیب‌پذیری	تعداد آسیب‌پذیری	تعداد آسیب‌پذیری با شدت بالا
اجرای کد	۵۰۲	۴۷۶
کسب امتیاز	۴۱۱	۳۰۸
کسب اطلاعات	۳۶۳	۳
سرریز	۲۶۵	۲۳۸
انکار سرویس	۱۹۵	۸۸
دور زدن محدودیت	۱۳۹	۸۱
تخریب حافظه	۸۸	۲۵
بقیه	۱۲	۲۳۸



شکل ۱۰- انواع آسیب‌پذیری‌های ویندوز سرور



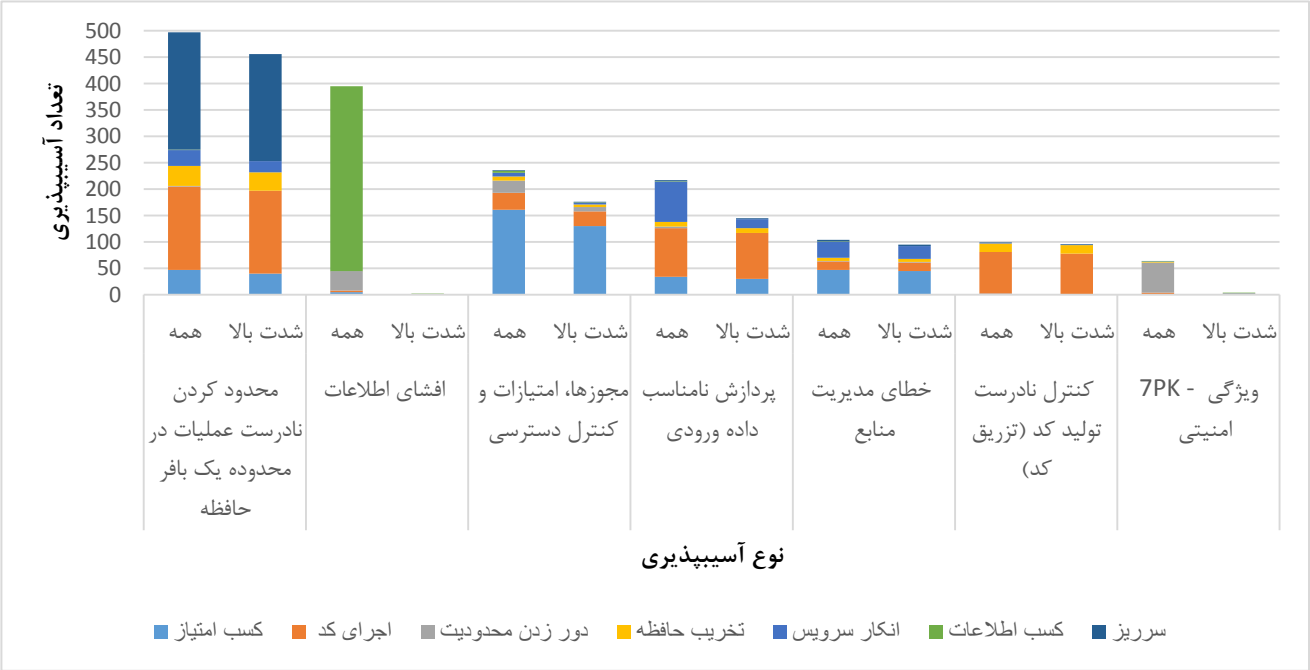
شکل ۱۱- انواع آسیب‌پذیری‌های باشدت بالای ویندوز سرور

جدول ۱۳ تاثیر انواع ضعف‌ها بر انواع آسیب‌پذیری‌ها را برای CVEهای ویندوز سرور با دو دسته‌بندی بدون شرط شدت و شدت بالا نمایش می‌دهد. بر اساس نتایج کسب شده بیشترین ضعف شناسایی شده در ویندوز سرورها محدود کردن

نادرست عملیات در یک بافر است. این ضعف موجب ایجاد ۴ نوع آسیب‌پذیری کسب امتیاز، اجرای کد، انکار سرویس و سرریز می‌شود. می‌توان گفت دلیل اصلی آسیب‌پذیری سرریز وجود ضعف از نوع "محدود کردن نادرست عملیات در محدوده یک بافر" می‌باشد. ضعف افشای اطلاعات دومین نوع ضعف دیده شده در ویندوز سرورها می‌باشد. این نوع ضعف در ۸۸٪ مواقع موجب آسیب‌پذیری کسب اطلاعات می‌باشد که در اکثر موارد شدت آسیب‌پذیری بالا نیست. ضعف "مجوزها، امتیازات و کنترل دسترسی" در ۶۸٪ مواقع موجب آسیب‌پذیری کسب امتیاز می‌شود. البته این نوع آسیب‌پذیری می‌تواند ناشی از دیگر ضعف‌ها نیز باشد. ضعف کنترل نادرست تولید کد در بسیاری از موارد موجب آسیب‌پذیری اجرای کد می‌شود. این نوع ضعف در ۹۹٪ موارد موجب ایجاد آسیب‌پذیری‌های با شدت بالا می‌شود. ضعف 7PK-ویژگی امنیتی نسبت به ضعف‌های دیگر اشاره شده کمتر در ویندوز سرورها وجود دارد. همچنین شدت آسیب‌پذیری‌های ناشی از این نوع ضعف در اکثر موارد بالا نیست.

جدول ۱۳- انواع آسیب‌پذیری‌ها بر اساس انواع ضعف‌ها

نوع آسیب‌پذیری	مجوزها، امتیازات کنترل دسترسی		افشای اطلاعات		محدود کردن نادرست عملیات		خطای مدیریت منابع		پردازش نامناسب داده ورودی		کنترل نادرست تولید کد		7PK - ویژگی امنیتی	
	همه	شدت بالا	همه	شدت بالا	همه	شدت بالا	همه	شدت بالا	همه	شدت بالا	همه	شدت بالا	همه	شدت بالا
کسب امتیاز	۱۶۱	۱۳۰	۵	۰	۴۷	۴۰	۴۷	۴۵	۳۴	۳۰	۲	۱	۱	۱
اجرای کد	۳۲	۲۸	۳	۰	۱۵۸	۱۵۷	۱۶	۱۶	۹۲	۸۷	۷۹	۷۷	۳	۰
دور زدن محدودیت	۲۳	۸	۳۵	۱	۱	۰	۱	۱	۳	۰	۰	۰	۵۷	۰
تخریب حافظه	۸	۵	۱	۰	۳۸	۳۵	۶	۶	۹	۹	۱۶	۱۶	۱	۰
انکار سرویس	۷	۳	۱	۰	۳۰	۲۱	۳۰	۲۴	۷۶	۱۷	۱	۱	۱	۱
کسب اطلاعات	۴	۱	۳۵۰	۱	۱	۰	۱	۰	۱	۰	۰	۰	۱	۰
سرریز	۱	۱	۰	۰	۲۲۲	۲۰۳	۳	۳	۲	۲	۱	۱	۰	۰



شکل ۱۲- انواع آسیب‌پذیری‌ها بر اساس انواع ضعف‌ها

۲-۴- بررسی کدهای بهره‌برداری عمومی منتشر شده برای ویندوز سرور

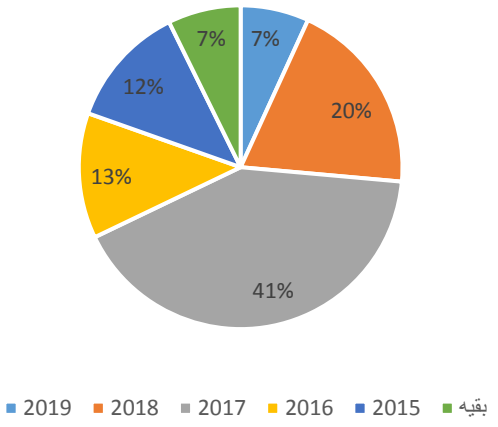
بر اساس نتایج حاصل از اطلاعات جمع‌آوری شده برای ۱۶٪ از آسیب‌پذیری‌های ویندوز سرور کد بهره‌برداری در پایگاه‌داده آسیب‌پذیری‌های مانند Exploit-db منتشر شده است که از این بین ۱۱۹ آسیب‌پذیری دارای شدت بالا، ۸۲ آسیب‌پذیری دارای شدت متوسط و ۸۰ آسیب‌پذیری دارای شدت پایین می‌باشند. ۹۳٪ از کدهای بهره‌برداری در ۴ سال اخیر منتشر شده است که این نشان از اهمیت بروزرسانی ویندوز سرورها دارد. کدهای بهره‌برداری منتشر شده در سال ۲۰۱۷ می‌باشد که در واقع در این سال بیشترین تعداد آسیب‌پذیری‌ها نیز منتشر شده بود. جدول ۱۴ فراوانی کدهای بهره‌برداری منتشر شده برای ویندوز سرور را به تفکیک سال‌ها نشان می‌دهد.

بر اساس ارزیابی‌ها مشخص گردید، همان‌طور که بیشترین تعداد آسیب‌پذیری‌های منتشر شده برای ویندوز ۲۰۰۸ می‌باشد، بیشترین تعداد کدهای بهره‌برداری منتشر شده نیز متعلق به این ویندوز سرور است. ۲۲۶ آسیب‌پذیری برای این ویندوز سرور منتشر شده که ۱۰۲ آسیب‌پذیری با شدت بالا، ۵۷ آسیب‌پذیری با شدت متوسط و ۶۷ آسیب‌پذیری با شدت پایین می‌باشند. ویندوز سرور ۲۰۱۲ در مرتبه دوم قرار دارد. حتی برای ویندوز سرور ۲۰۱۹ نیز ۲۰ کد بهره‌برداری منتشر شده

که از این بین ۵ مورد دارای شدت بالا بودند. جدول ۱۴ فراوانی کدهای بهره‌برداری بر اساس محصول و شدت آسیب‌پذیری را نمایش می‌دهد.

جدول ۱۴- فراوانی کد بهره برداری منتشر شده برای ویندوز سرور در طول سال‌ها

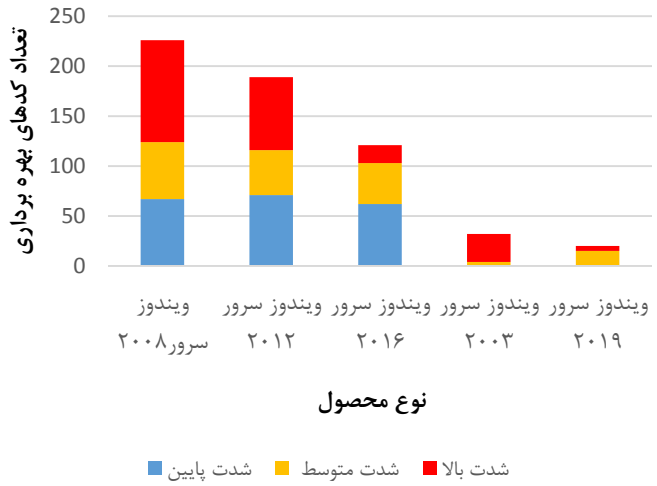
سال	تعداد کد بهره برداری
۲۰۱۵	۵۴
۲۰۱۶	۵۵
۲۰۱۷	۱۸۲
۲۰۱۸	۸۶
۲۰۱۹	۳۰
سایر	۳۲



شکل ۱۳- کد بهره‌برداری تولید شده در طول سال‌ها

جدول ۱۵- فراوانی کدهای بهره‌برداری بر اساس محصول و شدت آسیب‌پذیری

نام محصول	تعداد کد بهره برداری با شدت		
	پایین	متوسط	بالا
ویندوز سرور۲۰۰۸	۱۰۲	۵۷	۶۷
ویندوز سرور ۲۰۱۲	۷۳	۴۵	۷۱
ویندوز سرور ۲۰۱۶	۱۸	۴۱	۶۲
ویندوز سرور ۲۰۰۳	۲۸	۴	۰
ویندوز سرور ۲۰۱۹	۵	۱۴	۱



شکل ۱۴- فراوانی کد بهره‌برداری به تفکیک محصول و شدت آسیب-پذیری

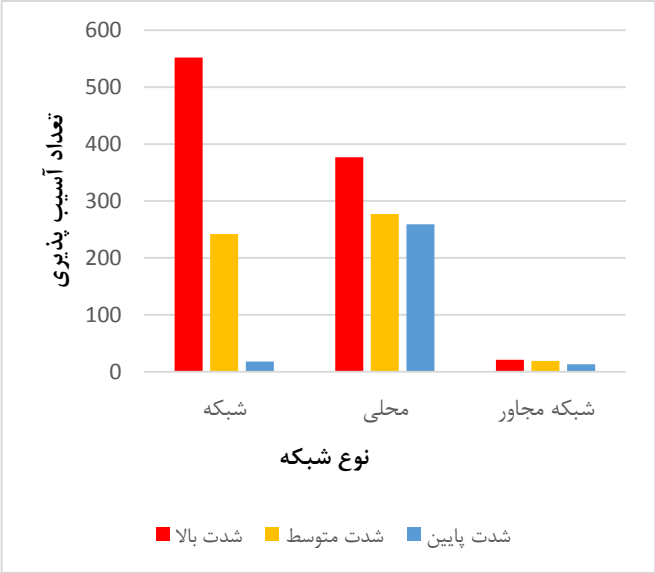
۲-۵- بررسی نحوه دسترسی به آسیب‌پذیری‌ها

نحوه دسترسی بیانگر چگونگی بهره‌برداری از یک آسیب‌پذیری می‌باشد. براساس تحقیقات انجام شده ۵۱٪ از آسیب‌پذیری-های ویندوز سرورها از طریق شبکه قابل دسترس بوده و از راه دور قابل بهره‌برداری می‌باشند. ۴۵٪ از آسیب‌پذیری‌ها، نیازمند دسترسی محلی هستند به این معنا که نفوذگر باید به صورت فزیکی به سیستم دسترسی داشته باشد یا دارای حساب‌کاربری محلی باشد و در ۵٪ موارد نفوذگر نیاز دارد برای بهره‌برداری در شبکه مجاور Adjacent Network سیستم هدف باشد.

در جدول ۱۶ قابل مشاهده است که بیش از ۵۸٪ از آسیب‌پذیری‌های با شدت بالا از طریق شبکه قابل دسترس هستند و این موضوع لزوم توجه به این آسیب‌پذیری‌ها را بسیار بیشتر می‌کند.

جدول ۱۶- نحوه دسترسی به آسیب‌پذیری

نحوه	شدت آسیب‌پذیری		
	بالا	متوسط	پایین
شبکه	۵۵۲	۲۴۲	۱۸
محلی	۳۷۷	۲۷۷	۲۵۹
شبکه مجاور	۲۱	۱۹	۱۳



شکل ۱۵- نحوه دسترسی به آسیب‌پذیری

بررسی نسخه‌های مختلف

۳-۱- ویندوز سرور ۲۰۰۸

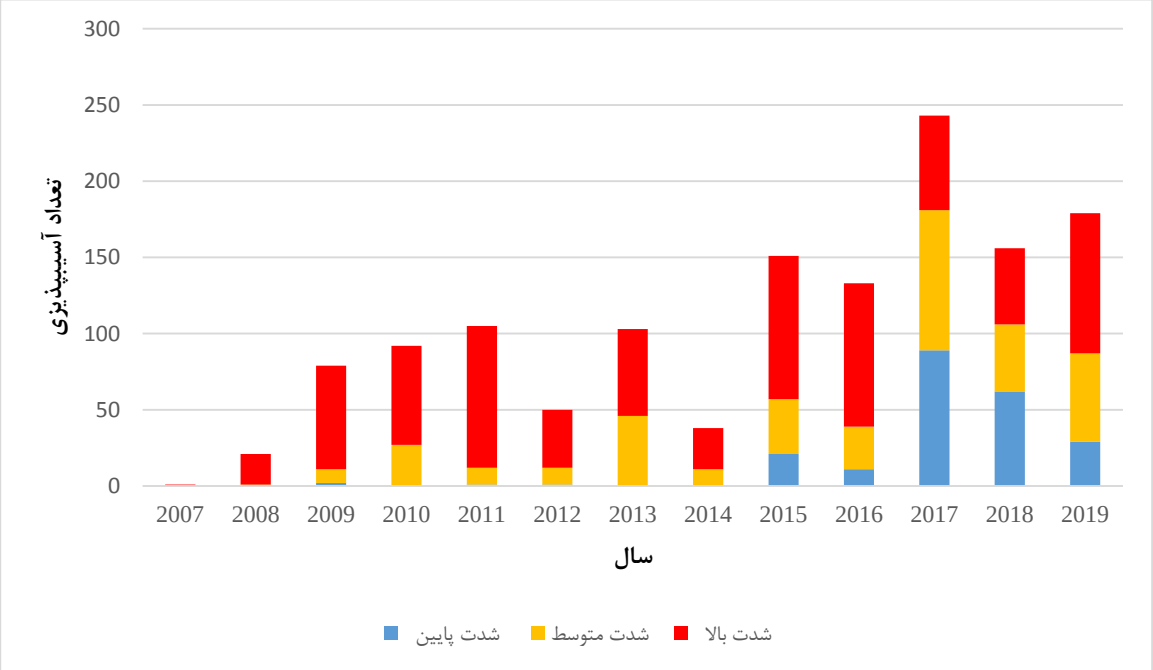
بر اساس تحقیقات انجام شده، ۲۴٪ سایت‌های دارای سیستم‌عامل ویندوز از ویندوز سرور ۲۰۰۸ استفاده می‌کنند. بیش از ۷۵٪ آسیب‌پذیری‌های بررسی شده، ویندوز سرور ۲۰۰۸ را تحت تاثیر قرار می‌دهد. با توجه به این‌که آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۸ در ۹۸٪ موارد شامل نسخه R2 می‌شود از بررسی مجدد این نسخه صرف نظر شده است و در واقع همین نتایج برای این نسخه نیز قابل تعمیم می‌باشند. تعداد زیاد وبسایت‌هایی که از ویندوز سرور ۲۰۰۸ استفاده می‌کنند، بسیار نگران‌کننده می‌باشد. زیرا اولا بر اساس بیانیه رسمی مایکروسافت پشتیبانی از این محصول از تاریخ ۱۴ فوریه سال ۲۰۲۰ انجام نخواهد شد و بروزرسانی برای آن منتشر نمی‌شود، دوما تعداد آسیب‌پذیری‌ها و کدهای بهره-برداری منتشر شده برای آن بسیار زیاد است و این احتمال بهره‌برداری از آسیب‌پذیری را افزایش می‌دهد.

جدول ۱۷ فراوانی آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۸ بر اساس شدت آسیب‌پذیری را نمایش می‌دهد. بر اساس نتایج حاصل از بررسی آسیب‌پذیری‌ها مشخص شد، ٪۵۶ از آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۸ دارای شدت بالا هستند.

از همان سال اول انتشار ویندوز سرور ۲۰۰۸، آسیب‌پذیری‌هایی برای این نسخه انتشار یافت تا سال ۲۰۱۴ اکثر آسیب-پذیرهای منتشر شده دارای شدت متوسط یا بالا بودند. اما در سال‌های اخیر تعداد آسیب‌پذیری‌های با سطح متوسط در حال افزایش می‌باشد. باتوجه به اینکه در نیمه‌های سال ۲۰۱۹ میلادی می‌باشیم، افزایش قابل ملاحظه در تعداد آسیب-پذیری‌ها منتشر شده برای این نسخه نسبت به سال پیش مشاهده می‌شود. آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۸ از روند کلی آسیب‌پذیرهای منتشر شده برای ویندوز سرورها پیروی می‌کند. در این محصول نیز به‌جز سال‌های ۲۰۱۲ و ۲۰۱۴ روند افزایشی تعداد آسیب‌پذیری‌ها قابل ملاحظه می‌باشد. حداکثر تعداد آسیب‌پذیری‌های منتشر شده برای این محصول در سال ۲۰۱۷ می‌باشد که به ۲۴۳ عدد رسیده است.

جدول ۱۷- فراوانی آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۸ بر اساس شدت آسیب‌پذیری

سال	تعداد آسیب‌پذیری		
	شدت بالا	شدت متوسط	شدت پایین
۲۰۰۷	۱	۰	۰
۲۰۰۸	۲۰	۱	۰
۲۰۰۹	۶۸	۹	۲
۲۰۱۰	۶۵	۲۷	۰
۲۰۱۱	۹۳	۱۱	۱
۲۰۱۲	۳۸	۱۱	۱
۲۰۱۳	۵۷	۴۶	۰
۲۰۱۴	۲۷	۱۱	۰
۲۰۱۵	۹۴	۳۶	۲۱
۲۰۱۶	۹۴	۲۸	۱۱
۲۰۱۷	۶۲	۹۲	۸۹
۲۰۱۸	۵۰	۴۴	۶۲
۲۰۱۹	۹۲	۵۸	۲۹

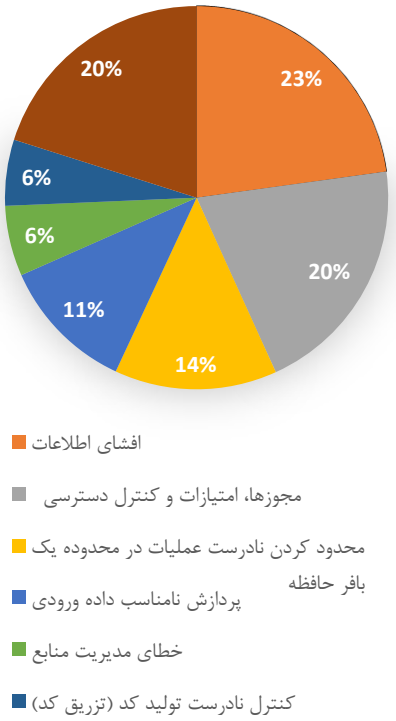


شکل ۱۶- فراوانی آسیب‌پذیری‌های منتشر شده برای ویندوز سرور براساس شدت

بر اساس ارزیابی داده‌های موجود، ۲۳٪ از آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۸ از نوع ضعف افشای اطلاعات می‌باشند و ۲۰٪ از نوع مجوزها، امتیازات و کنترل دسترسی می‌باشند. ۸۰٪ از آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۸ در ۶ دسته ضعف قراردارند. در مقایسه انواع آسیب‌پذیری‌های ویندوز سرور متوجه می‌شویم که ضعف افشای اطلاعات در این ویندوز به رتبه اول رسیده است. با این حال روند کلی ضعف‌ها برای ویندوز سرور ۲۰۰۸ همانند همه ویندوز سرورها می‌باشد.

جدول ۱۸- انواع ضعف ویندوز سرور ۲۰۰۸

نوع ضعف	تعداد آسیب‌پذیری
افشای اطلاعات	۳۱۱
مجوزها، امتیازات و کنترل دسترسی	۲۷۸
محدود کردن نادرست عملیات در محدوده یک بافر حافظه	۱۸۷
پردازش نامناسب داده ورودی	۱۵۶
خطای مدیریت منابع	۸۱
کنترل نادرست تولید کد (تزریق کد)	۷۶
سایر	۲۷۴



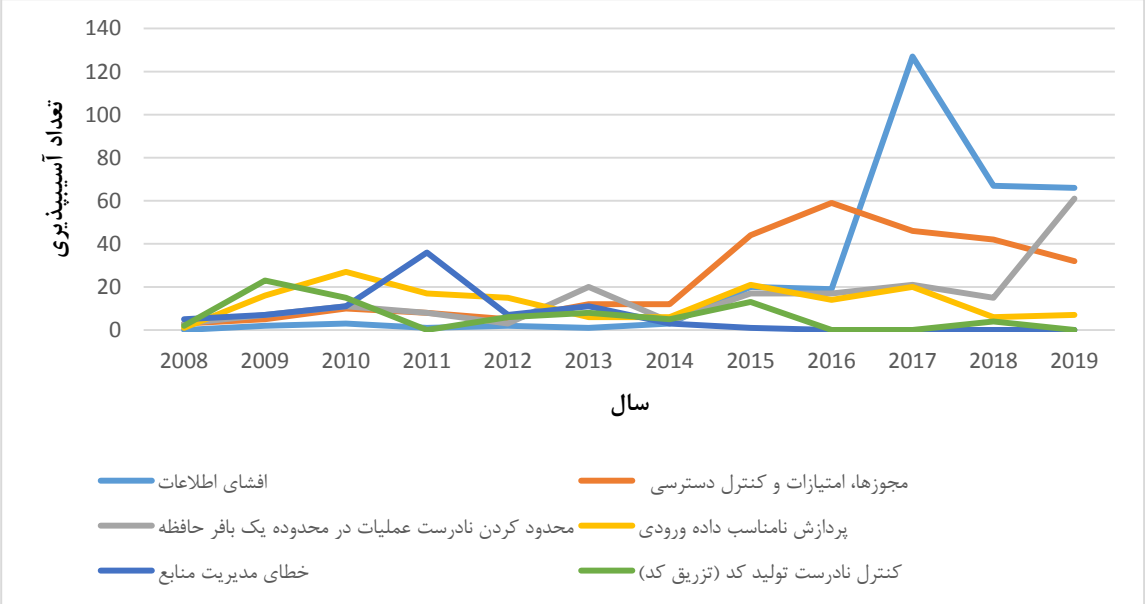
شکل ۱۷- انواع ضعف ویندوز سرور ۲۰۰۸

چگونگی تغییر روند نوع ضعف ویندوز سرور ۲۰۰۸ در طول سال‌ها نشان می‌دهد که بیشترین تغییرات در طول سال‌ها متوجه آسیب‌پذیری افشای اطلاعات بوده است. این آسیب‌پذیری در سال ۲۰۱۷ به اوج رسیده و سپس روند رو به پایینی را پیش گرفته است و احتمالا در سال ۲۰۱۹ مجدد افزایش نسبی نسبت به سال‌های قبل خواهد داشت. آسیب‌پذیری از نوع ضعف "محدود کردن نادرست عملیات در محدوده یک بافر حافظه" به صورت ملایم در حال نوسان بوده است. اما در سال اخیر دارای جهش با شیب تند می‌باشد.

جدول ۱۹- تغییرات فراوانی آسیب‌پذیری‌های ویندوز سرور ۲۰۰۸ بر اساس ضعف

سال	افشای اطلاعات	مجوزها، امتیازات و کنترل دسترسی	محدود کردن نادرست عملیات	پردازش نامناسب داده ورودی	خطای مدیریت منابع	کنترل نادرست تولید کد
۲۰۰۸	۰	۳	۳	۱	۵	۲

۲۰۰۹	۲	۵	۷	۱۶	۷	۲۳
۲۰۱۰	۳	۱۰	۱۱	۲۷	۱۱	۱۵
۲۰۱۱	۱	۸	۸	۱۷	۳۶	۰
۲۰۱۲	۲	۵	۳	۱۵	۷	۶
۲۰۱۳	۱	۱۲	۲۰	۶	۱۱	۸
۲۰۱۴	۳	۱۲	۴	۶	۳	۵
۲۰۱۵	۲۰	۴۴	۱۷	۲۱	۱	۱۳
۲۰۱۶	۱۹	۵۹	۱۷	۱۴	۰	۰
۲۰۱۷	۱۲۷	۴۶	۲۱	۲۰	۰	۰
۲۰۱۸	۶۷	۴۲	۱۵	۶	۰	۴
۲۰۱۹	۶۶	۳۲	۶۱	۷	۰	۰



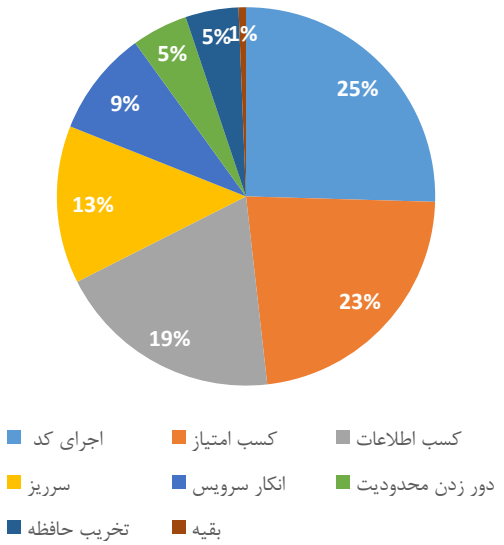
شکل ۱۸- تغییرات فراوانی آسیب‌پذیری‌های ویندوز سرور ۲۰۰۸ بر اساس ضعف

در جدول ۲۰ تاثیر شدت آسیب‌پذیری‌های ویندوز سرور ۲۰۰۸ بر روی نوع آسیب‌پذیری‌های این سیستم‌عامل بررسی شده است. ۲۵٪ از انواع آسیب‌پذیری‌های ویندوز سرور ۲۰۰۸ را اجرای کد از راه دور تشکیل می‌دهد. درحالی‌که اگر فقط آسیب‌پذیری‌ها با شدت بالا را در نظر بگیریم این میزان به ۳۸٪ تغییر خواهد کرد و این موضوع از اهمیت بالای این نوع ضعف در ویندوز سرور ۲۰۰۸ خبر می‌دهد. همان طورکه در روند کلی ویندوزها نیز قابل مشاهده بود، ضعف کسب اطلاعات

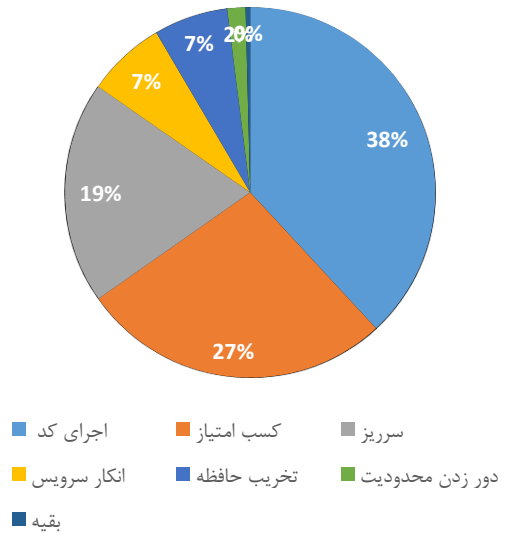
در انواع آسیب‌پذیری‌ها با شدت بالا وجود ندارد. دومین نوع آسیب‌پذیری‌ها تاثیرگذار در این ویندوز سرور کسب امتیاز می‌باشد که در ۳۶۱ آسیب‌پذیری دیده شده است.

جدول ۲۰- فراوانی انواع آسیب‌پذیری ویندز سرور ۲۰۰۸

نوع آسیب‌پذیری	همه آسیب‌پذیری ویندوز ۲۰۰۸	آسیب پذیری های با شدت بالا ویندوز ۲۰۰۸
اجرای کد	۴۰۴	۳۸۳
کسب امتیاز	۳۶۱	۲۷۳
کسب اطلاعات	۳۰۷	ناچیز
سرریز	۲۱۴	۱۹۵
انکار سرویس	۱۴۳	۶۹
دور زدن محدودیت	۷۶	۱۶
تخریب حافظه	۷۲	۶۵
بقیه	۱۰	۴



شکل ۱۹- انواع آسیب‌پذیری ویندوز سرور ۲۰۰۸ بر اساس آسیب‌پذیری‌هایی با شدت بالا



شکل ۲۰- انواع آسیب‌پذیری‌های ویندوز سرور ۲۰۰۸

۳-۲- ویندوز سرور ۲۰۱۲

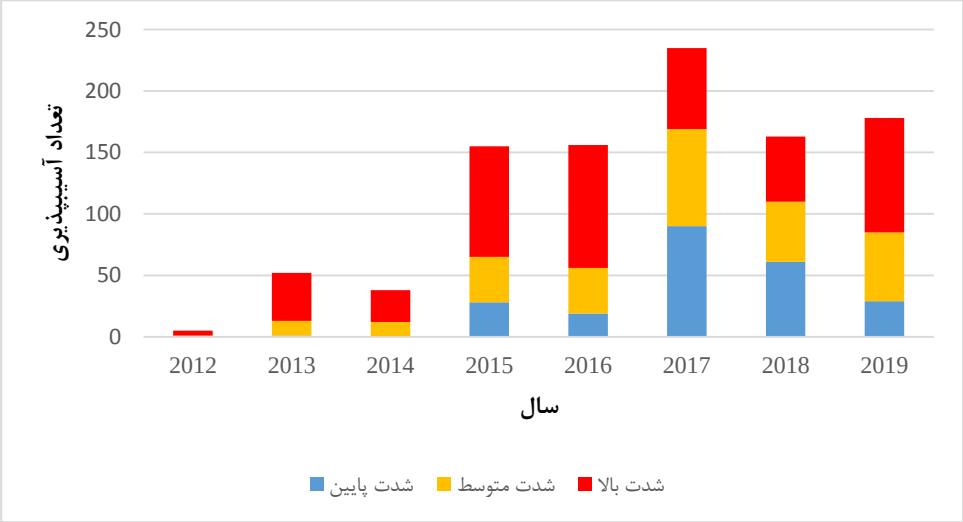
بر اساس گزارش تکنولوژی‌های ساخت استفاده شده در فضای وب کشور، ۳۹٪ از ویندوز سرورهای شناسایی شده کشور را ویندوز سرور ۲۰۱۲ تشکیل می‌دهد که پر استفاده‌ترین ویندوز سرور کشور می‌باشد. یکی از معروف‌ترین نسخه‌های این ویندوز سرور نسخه 2012 R2 می‌باشد. با توجه به مقادیر جدول ۲۱، ۹۱۸ آسیب‌پذیری برای این ویندوز سرور منتشر شده است که ۵۵٪ از کل آسیب‌پذیری‌های شناسایی شده را شامل می‌شود. بررسی‌های اولیه نشان می‌دهد که ۹۴٪ از آسیب-پذیری‌های منتشر شده برای ویندوز سرور ۲۰۱۲ نسخه 2012 R2 را نیز تحت تاثیر قرار می‌دهند. اما با بررسی بیشتر دریافتیم که در واقع ۵٪ از آسیب‌پذیری‌ها قبل از انتشار نسخه 2012 R2 شناسایی شدند و درصد همپوشانی با آسیب-پذیری‌های بعد از این تاریخ ۹۹٪ می‌باشد.

بر اساس بررسی‌های انجام شده از همان سال اول انتشار ویندوز ۲۰۱۲، آسیب‌پذیری‌هایی نیز برای آن منتشر شد. در سال ۲۰۱۲ چهار آسیب‌پذیری با شدت بالا و یک آسیب‌پذیری با شدت متوسط برای این ویندوز سرور انتشار یافت. در سال ۲۰۱۳ تعداد آسیب‌پذیری‌ها به شدت افزایش یافته و ۳۹ آسیب‌پذیری با شدت بالا (در همین سال فقط ۵ آسیب‌پذیری با شدت بالا برای ویندوز سرور 2012 R2 منتشر شده است.) منتشر شد. سپس تعداد آسیب‌پذیری‌های منتشر شده در سال ۲۰۱۴ کاهش یافت. برای سال‌های بعد، افزایش نسبی در تعداد آسیب‌پذیری‌ها دیده می‌شود؛ به طوریکه تعداد آسیب‌پذیری‌های منتشر شده در سال ۲۰۱۷ به حداکثر رسید و ۲۳۵ آسیب‌پذیری در این سال منتشر شد. اما نکته مهم در سال ۲۰۱۷ کاهش تعداد آسیب‌پذیری‌های با شدت بالا نسبت به سال‌های قبل می‌باشد. در سال ۲۰۱۸ آسیب‌پذیری‌ها نسبت به سال ۲۰۱۷ قبل کاهش یافت. در حال حاضر با این‌که فقط نیمی از سال ۲۰۱۹ گذشته تعداد آسیب‌پذیری‌ها نسبت به سال‌های قبل بیشتر شده و ۹۳ آسیب‌پذیری بحرانی در سال ۲۰۱۹ منتشر شده است.

جدول ۲۱- شدت آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۱۲

سال انتشار آسیب پذیری	تعداد آسیب‌پذیری		
	شدت بالا	شدت متوسط	شدت پایین
۲۰۱۲	۴	۱	۰
۲۰۱۳	۳۹	۱۲	۱
۲۰۱۴	۲۶	۱۲	۰
۲۰۱۵	۹۰	۳۷	۲۸

۲۰۱۶	۱۰۰	۳۷	۱۹
۲۰۱۷	۶۶	۷۹	۹۰
۲۰۱۸	۵۳	۴۹	۶۱
۲۰۱۹	۹۳	۵۶	۲۹

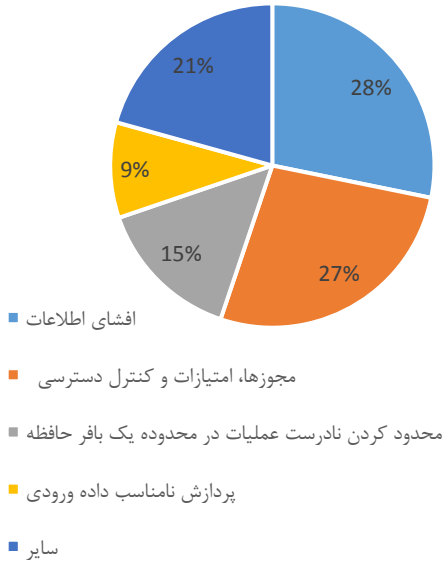


شکل ۲۱- شدت آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۱۲

نتایج حاصل از بررسی‌ها نشان می‌دهد که ضعف افشای اطلاعات بیشترین سهم را در میان ضعف‌های ویندوز سرور ۲۰۱۲ دارد و در ۲۷۸ آسیب‌پذیری دیده شده است. ضعف مجوزها، امتیازات و کنترل دسترسی دومین نوع ضعف عمده این سیستم عامل می‌باشد و در ۲۷۶ آسیب‌پذیری مورد سوء استفاده واقع شده است. نکته قابل توجه این است که ۷۹٪ از انواع ضعف‌های ویندوز سرور ۲۰۱۲ در چهار دسته‌بندی مجوزها، امتیازات و کنترل دسترسی، افشای اطلاعات، محدود کردن نادرست عملیات در محدوده یک بافر حافظه، پردازش نامناسب داده ورودی قرار دارند. با استناد به نتایج، انواع ضعف در ویندوز سرور ۲۰۱۲ R2 مشابه ویندوز سرور ۲۰۱۲ می‌باشد. انواع ضعف‌های این سیستم‌عامل در جدول ۲۲ نمایش داده شده است.

جدول ۲۲- فراوانی انواع ضعف‌های ویندوز ۲۰۱۲

نوع ضعف	تعداد آسیب‌پذیری
افشای اطلاعات	۲۷۸
مجوزها، امتیازات و کنترل دسترسی	۲۶۶
محدود کردن نادرست عملیات	۱۴۴
پردازش نامناسب داده ورودی	۹۴
سایر	۲۰۴



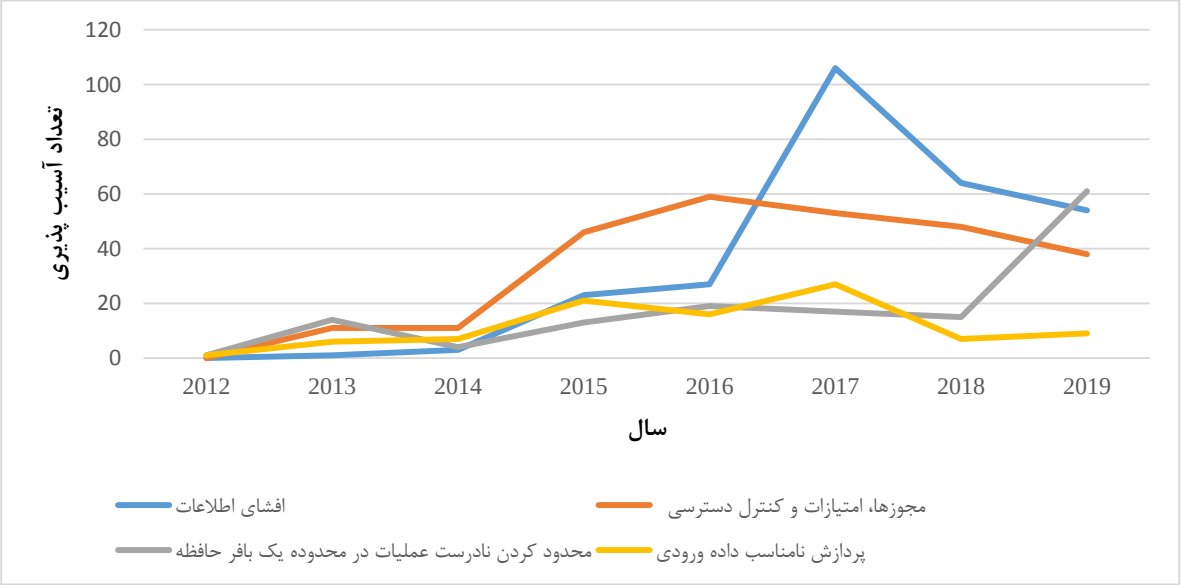
شکل ۲۲- انواع ضعف‌های ویندوز سرور ۲۰۱۲

بر اساس نتایج قابل مشاهده در جدول ۲۳ انواع ضعف‌های ویندوز سرور ۲۰۱۲ در طول سال‌ها دچار تغییرات زیادی شده است. روند رو به رشد انواع ضعف‌ها، مخصوصا در سال‌های اولیه انتشار ویندوز ۲۰۱۲ قابل مشاهده است. نوع ضعف مجوزها، امتیازات و کنترل دسترسی تا سال ۲۰۱۶ بیشترین نوع ضعف بوده است؛ اما در سال‌های اخیر تعداد آسیب‌پذیری‌های کشف شده از این نوع کاهش یافته است. نوع ضعف افشای اطلاعات نیز روند مشابهی را طی کرده و تا سال ۲۰۱۷ با افزایش تعداد مواجه بوده ولی در دو سال اخیر تعداد آسیب‌پذیری‌ها کاهش یافته است. روند تغییرات برای ویندوز سرور R2 2012 دقیقا مشابه همین مورد می‌باشد؛ با این تفاوت که تعداد آسیب‌پذیری‌ها در سال ۲۰۱۳ کمتر بوده و تنها ۴ مورد ضعف پردازش نامناسب داده ورودی و یک ضعف محدود کردن نادرست عملیات در محدوده یک بافر حافظه دیده شده است.

جدول ۲۳ – فراوانی ضعف‌های مختلف ویندوز سرور ۲۰۱۲ در طول سال‌ها

سال انتشار	افشای اطلاعات	مجوزها، امتیازات و کنترل دسترسی	محدود کردن نادرست عملیات در محدوده یک بافر حافظه	پردازش نامناسب داده ورودی
۲۰۱۲	۰	۰	۱	۱
۲۰۱۳	۱	۱۱	۱۴	۶
۲۰۱۴	۳	۱۱	۴	۷
۲۰۱۵	۲۳	۴۶	۱۳	۲۱

۲۰۱۶	۲۷	۵۹	۱۹	۱۶
۲۰۱۷	۱۰۶	۵۳	۱۷	۲۷
۲۰۱۸	۶۴	۴۸	۱۵	۷
۲۰۱۹	۵۴	۳۸	۶۱	۹



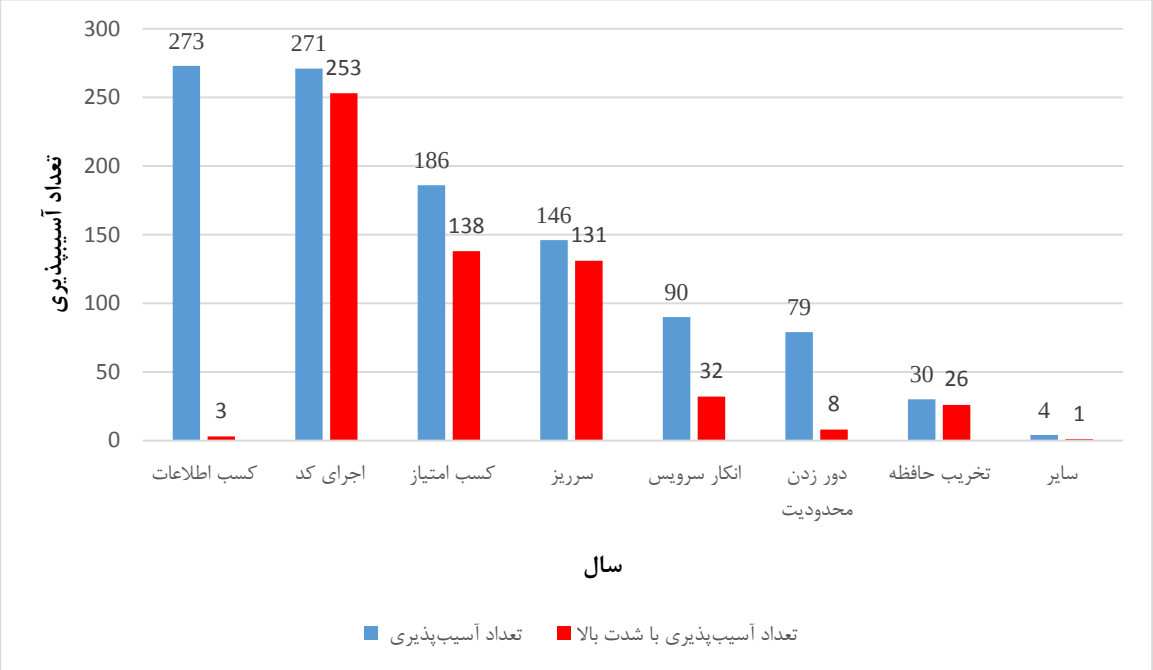
شکل ۲۳- روند تغییر انواع ضعف ویندوز سرور ۲۰۱۲

هنگام بررسی تاثیر شدت آسیب‌پذیری‌های ویندوز سرور ۲۰۱۲ بر روی انواع آسیب‌پذیری‌ها متوجه شدیم که در این ویندوز سرور نیز فراوانی نوع آسیب‌پذیری کسب اطلاعات بیشتر از دیگر انواع آسیب‌پذیری‌ها می‌باشد. همچنین فراوانی این نوع در هنگام بررسی آسیب‌پذیری با شدت بالا به حداقل می‌رسد. دومین نوع آسیب‌پذیری اجرای کد می‌باشد، این آسیب-پذیری در ۹۳٪ موارد دارای شدت بالا می‌باشد.

جدول ۲۴- تاثیر شدت آسیب‌پذیری‌های ویندوز ۲۰۱۲ بر روی انواع آسیب‌پذیری‌ها

نوع آسیب‌پذیری	تعداد آسیب‌پذیری	تعداد آسیب‌پذیری با شدت بالا
کسب اطلاعات	۲۷۳	۳
اجرای کد	۲۷۱	۲۵۳
کسب امتیاز	۱۸۶	۱۳۸

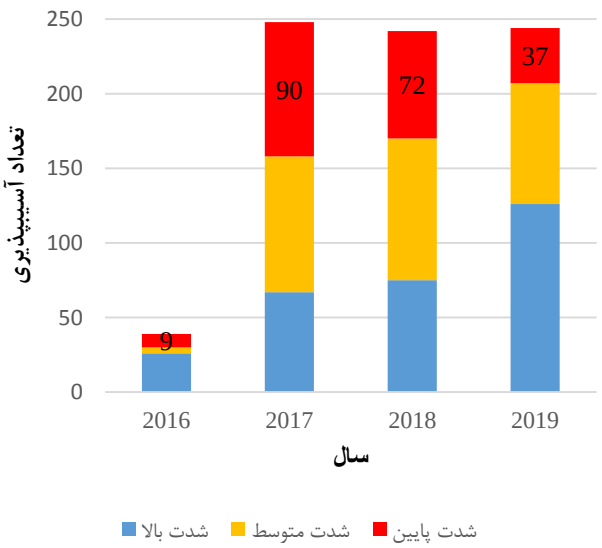
سرریز	۱۴۶	۱۳۱
انکار سرویس	۹۰	۳۲
دور زدن محدودیت	۷۹	۸
تخریب حافظه	۳۰	۲۶
سایر	۴	۱



شکل۲۴- تاثیر شدت آسیب‌پذیری‌های ویندوز ۲۰۱۲ بر روی انواع آسیب‌پذیری‌ها

۳-۳- ویندوز سرور ۲۰۱۶

براساس ارزیابی‌های انجام شده فراوانی آسیب‌پذیری منتشر شده برای ویندوز سرور ۲۰۱۶ در مقایسه با دیگر ویندوز سرورها بیشتر بوده است. در سال اول انتشار این ویندوز سرور ۳۹ آسیب‌پذیری برای آن منتشر شد که ۲۶ آسیب‌پذیری دارای شدت بالا بود. تعداد آسیب‌پذیری‌های منتشر شده در سال ۲۰۱۷ به شدت افزایش یافت. در این سال حدود ۲۵۰ آسیب-پذیری برای این ویندوز سرور منتشر شد که این میزان بیشترین تعداد آسیب‌پذیری‌های منتشر شده برای یک ویندوز سرور می‌باشد. با وجود عدم افزایش تعداد آسیب‌پذیری‌ها در سال‌های اخیر تعداد آسیب‌پذیری‌های با شدت بالا همواره در حال افزایش بوده است. جدول ۲۵ فراوانی آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۱۶ را نمایش می‌دهد.



شکل۲۵- شدت آسیب‌پذیری منتشر شده برای ویندوز سرور ۲۰۱۶

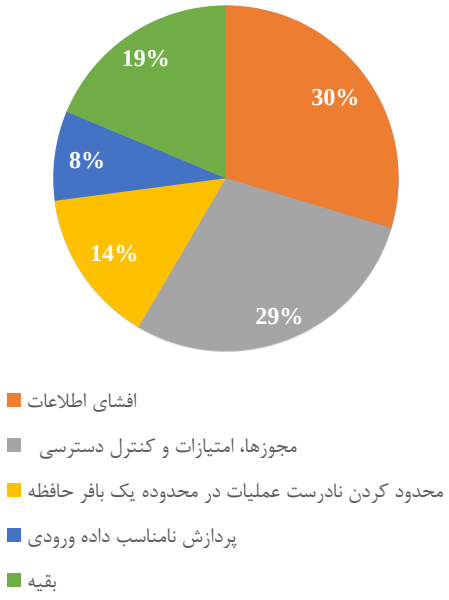
جدول ۲۵- شدت آسیب‌پذیری منتشر شده برای ویندوز سرور ۲۰۱۶

	تعداد آسیب‌پذیری‌ها با شدت		
	بالا	متوسط	پایین
۲۰۱۶	۲۶	۴	۹
۲۰۱۷	۶۷	۹۱	۹۰
۲۰۱۸	۷۵	۹۵	۷۲
۲۰۱۹	۱۲۶	۸۱	۳۷

بر اساس بررسی‌های انجام شده، تقریبا ۸۰٪ از انواع ضعف‌های ویندوز سرور ۲۰۱۶ از چهار نوع ضعف تشکیل شده است که به ترتیب ۳۰٪ از نوع افشای اطلاعات، ۲۹٪ از نوع ضعف مجوزها امتیازات و کنترل دسترسی، ۱۴٪ از نوع محدود کردن نادرست عملیات در محدوده یک بافر و ۸٪ از نوع پردازش نادرست داده‌های ورودی می‌باشند. جدول ۲۶ فراوانی انواع ضعف‌ها در ویندوز سرور ۲۰۱۶ را نمایش می‌دهد.

جدول ۲۶- فراوانی انواع ضعف ویندوز سرور ۲۰۱۶

انواع ضعف	تعداد آسیب‌پذیری
افشای اطلاعات	۲۳۰
مجوزها، امتیازات و کنترل دسترسی	۲۲۳
محدود کردن نادرست عملیات در محدوده یک بافر حافظه	۱۱۲
پردازش نامناسب داده ورودی	۶۵
بقیه	۱۴۵

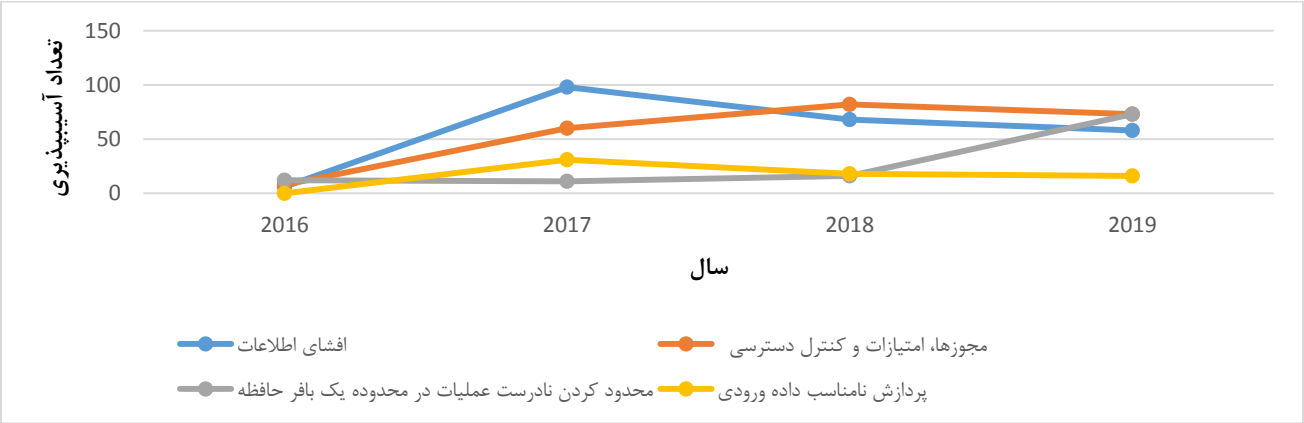


شکل ۲۶- انواع ضعف ویندوز سرور ۲۰۱۶

بر اساس داده‌های جدول ۲۷ تعداد همه ضعف‌ها به جز ضعف محدود کردن نادرست عملیات، افزایش یافته است. این ضعف تا سال ۲۰۱۸ تغییر چندانی نداشته اما در سال ۲۰۱۹ ، ۷۳ آسیب‌پذیری از این نوع ضعف منتشر شده است که نشان از بحرانی بودن این ضعف در سال جاری دارد.

جدول ۲۷- روند تغییر انواع ضعف‌های ویندوز سرور ۲۰۱۶

سال	افشای اطلاعات	مجوزها، امتیازات و کنترل دسترسی	محدود کردن نادرست عملیات در محدوده یک بافر حافظه	پردازش نامناسب داده ورودی
۲۰۱۶	۶	۸	۱۲	۰
۲۰۱۷	۹۸	۶۰	۱۱	۳۱
۲۰۱۸	۶۸	۸۲	۱۶	۱۸
۲۰۱۹	۵۸	۷۳	۷۳	۱۶

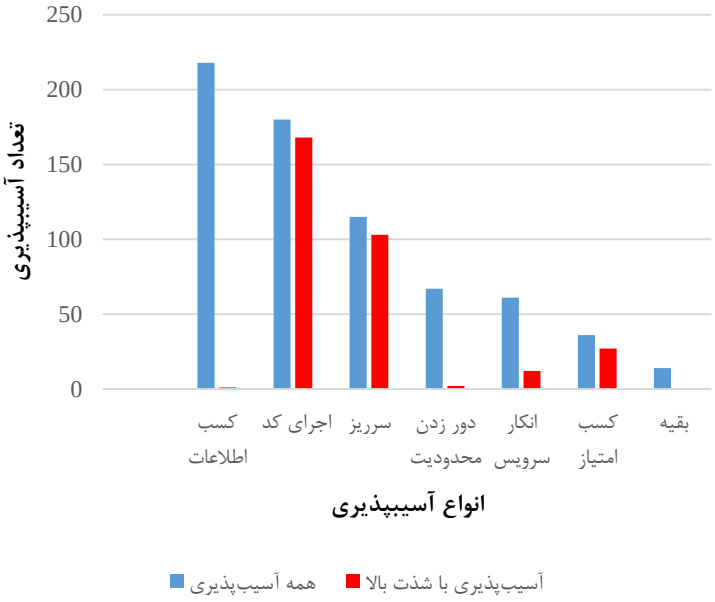


شکل ۲۷- روند تغییر انواع ضعف‌های ویندوز سرور ۲۰۱۶

بررسی تاثیر شدت آسیب‌پذیری بر روی نوع آسیب‌پذیری‌ها نشان می‌دهد که در ویندوز سرور ۲۰۱۶ نیز نوع آسیب‌پذیری-های افشای اطلاعات با ۳۱٪ در صدر انواع آسیب‌پذیری‌های منتشر شده قرار دارد. اما زمانی که فقط آسیب‌پذیری‌ها با شدت بالا در نظرگرفته می‌شوند این نوع آسیب‌پذیری به ۰٪ کاهش می‌یابد. تعداد CVEهای دو نوع آسیب‌پذیری دور زدن محدودیت و انکار سرویس نیز زمانی‌که فقط آسیب‌پذیری‌های با شدت بالا را در نظر می‌گیریم، کاهش می‌یابند. در مقابل بیشتر CVEهای منتشر شده از نوع اجرای کد و سرریز داری شدت بالا هستند و تفاوت چندانی در تعداد همه آسیب-پذیری‌ها و آسیب‌پذیری با شدت بالا دیده نمی‌شود. در جدول ۲۸ خلاصه مطالب فوق نمایش داده شده است.

جدول ۲۸- بررسی تاثیر شدت آسیب‌پذیری‌های بر روی انواع آسیب‌پذیری‌ها در ویندوز ۲۰۱۶

نوع آسیب‌پذیری	همه آسیب‌پذیری ویندوزسرور ۲۰۱۶	آسیب‌پذیری با شدت بالا ویندوزسرور ۲۰۱۶
کسب اطلاعات	۲۱۸	۱
اجرای کد	۱۸۰	۱۶۸
سرریز	۱۱۵	۱۰۳
دور زدن محدودیت	۶۷	۲
انکار سرویس	۶۱	۱۲
کسب امتیاز	۳۶	۲۷
بقیه	۱۴	۰



شکل ۲۸- بررسی تاثیر شدت آسیب‌پذیری‌ها بر روی انواع آسیب‌پذیری‌ها

۳-۴- ویندوز سرور ۲۰۰۳

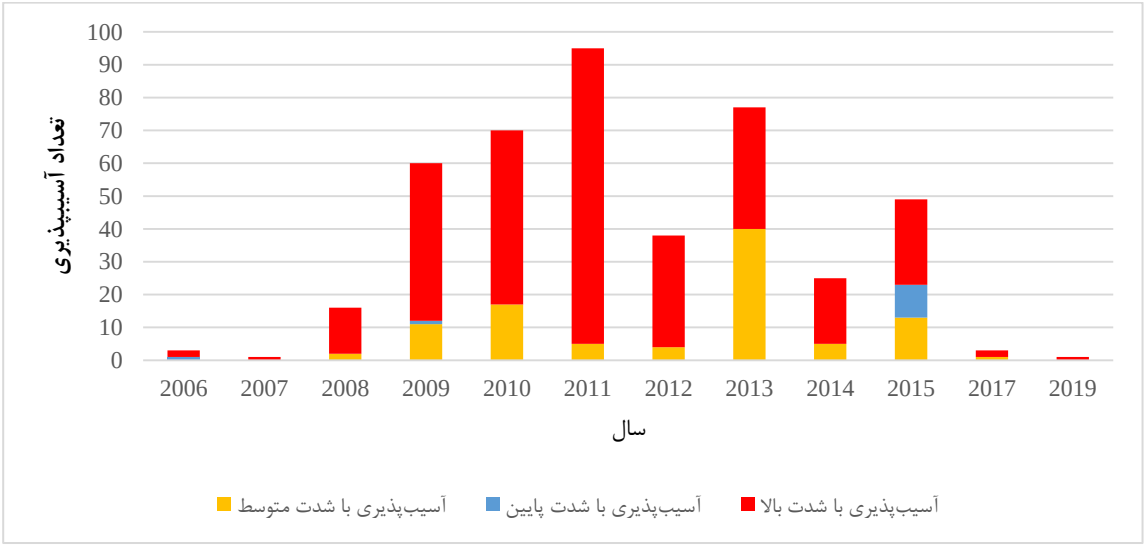
براساس بررسی‌های انجام شده، ویندوز سرور ۲۰۰۳، ۳٪ از ویندوز سرورهای استفاده شده در کشور را تشکیل می‌دهد. استفاده از این ویندوز سرور بسیار خطرناک می‌باشد. چراکه مایکروسافت پشتیبانی از این ویندوز سرور را در سال ۲۰۱۵ متوقف کرده است. بنابراین برای آسیب‌پذیری‌هایی که بعد از سال ۲۰۱۵ شناسایی شدند هیچ راه‌حل و بروزرسانی ارائه نشده است. این درحالیست که ۷۵٪ از آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۳ دارای شدت بالا هستند و این ویندوز سرور کمترین میزان آسیب‌پذیری‌های منتشر شده با شدت پایین را دارد.

اولین آسیب‌پذیری منتشر شده برای این ویندوز سرور متعلق به سال ۲۰۰۶ می‌باشد و تعداد آسیب‌پذیری‌های منتشر شده تا سال ۲۰۱۱ به شدت در حال افزایش بوده است. ولی در سال ۲۰۱۲ با کاهش چشم‌گیری به ۳۸ آسیب‌پذیری می‌رسد. در طی سال‌های بعد تعداد آسیب‌پذیری‌ها با تغییرات زیادی روبه‌رو می‌شود و در سال‌های اخیر روند کاهش آسیب‌پذیری‌ها قابل ملاحظه است، به نوعی که در سال ۲۰۱۸ هیچ آسیب‌پذیری برای این ویندوز منتشر نشده است. نکته مهم در مورد این ویندوز سرور تعداد زیاد آسیب‌پذیری‌ها با شدت بالا می‌باشد؛ به‌طوری‌که در اکثر سال‌ها تمام آسیب‌پذیری‌های منتشر شده،

دارای اهمیت بالا یا متوسط هستند. با وجود این‌که تعداد آسیب‌پذیری‌های منتشر شده در سال‌های اخیر برای این ویندوز سرور کاهش یافته ولی این موضوع از امنیت این ویندوز سرور ناشی نمی‌شود بلکه از اهمیت پایین این نوع ویندوز سرور برای محققان امنیتی خبر می‌دهد؛ چرا که مایکروسافت پشتیبانی از این ویندوز سرور را متوقف کرده است. بنابراین حتی تعداد کم آسیب‌پذیری‌های منتشر شده برای این ویندوز سرور بسیار خطرناک هستند زیرا بروزرسانی برای رفع آنها ارائه نمی‌شود.

جدول ۲۹- فراوانی شدت آسیب‌پذیری‌های منتشر شده برای ویندوز ۲۰۰۳

سال	آسیب‌پذیری با شدت بالا	آسیب‌پذیری با شدت متوسط	آسیب‌پذیری با شدت پایین
۲۰۰۶	۲	۰	۰
۲۰۰۷	۱	۰	۰
۲۰۰۸	۱۴	۲	۰
۲۰۰۹	۴۸	۱۱	۱
۲۰۱۰	۵۳	۱۷	۰
۲۰۱۱	۹۰	۵	۰
۲۰۱۲	۳۴	۴	۰
۲۰۱۳	۳۷	۴۰	۰
۲۰۱۴	۲۰	۵	۰
۲۰۱۵	۲۶	۱۳	۱۰
۲۰۱۷	۲	۱	۰
۲۰۱۹	۱	۰	۰

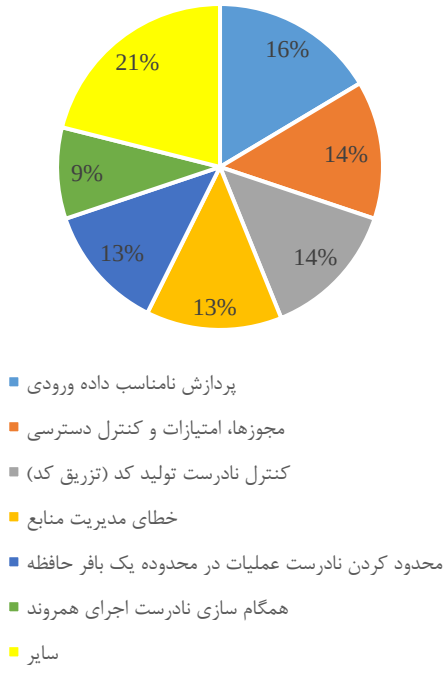


شکل۲۹- فراوانی شدت آسیب‌پذیری‌های منتشر شده برای ویندوز ۲۰۰۳

براساس مطالعات انجام شده، ۷۹٪ از CVEهای منتشر شده برای ویندوز ۲۰۰۳ در ۶ نوع ضعف دسته‌بندی می‌شوند. ضعف پردازش نامناسب داده ورودی با ۶۷ آسیب‌پذیری پر تکرارترین نوع ضعف می‌باشد. در مقابل ضعف همگام‌سازی نادرست اجرای همروند با ۳۷ آسیب‌پذیری در رتبه ششم قرار دارد. همان‌طورکه قابل مشاهده است، نوع ضعف پردازش نامناسب داده ورودی بر خلاف نمودار کلی ویندوز سرورها در این نوع سرور موجب ایجاد آسیب‌پذیری‌های زیادی شده است. همچنین در این ویندوز سرور ضعف همگام‌سازی نادرست اجرای همروند با نام CWE-362 قابل مشاهده است که به دلیل تاثیر بسیار کم در کل ویندوز سرورها در نمودار ضعف ویندوز سرورها نمایش داده نشده است. با توجه به تعداد زیاد آسیب‌پذیری‌ها با شدت بالا، تغییرات زیادی در نمودار ضعف‌های سیستم در صورتی که فقط آسیب‌پذیری‌ها با شدت بالا را در نظر بگیریم، رخ نمی-دهد. اما برخی از نوع ضعف‌ها مانند ضعف کنترل نادرست تولید کد، درصد بیشتری را دریافت می‌کنند که این نشان از شدت بالای آسیب‌پذیری‌های از این نوع ضعف می باشد.

جدول ۳۰- فراوانی انواع ضعف‌های ویندوز سرور ۲۰۰۳

نوع ضعف	تعداد آسیب‌پذیری
پردازش نامناسب داده ورودی	۶۷
مجوزها، امتیازات و کنترل دسترسی	۵۶
کنترل نادرست تولید کد (تزریق کد)	۵۶
خطای مدیریت منابع	۵۵
محدود کردن نادرست عملیات در محدوده یک بافر حافظه	۵۱
همگام سازی نادرست اجرای همروند	۳۷
سایر	۸۶

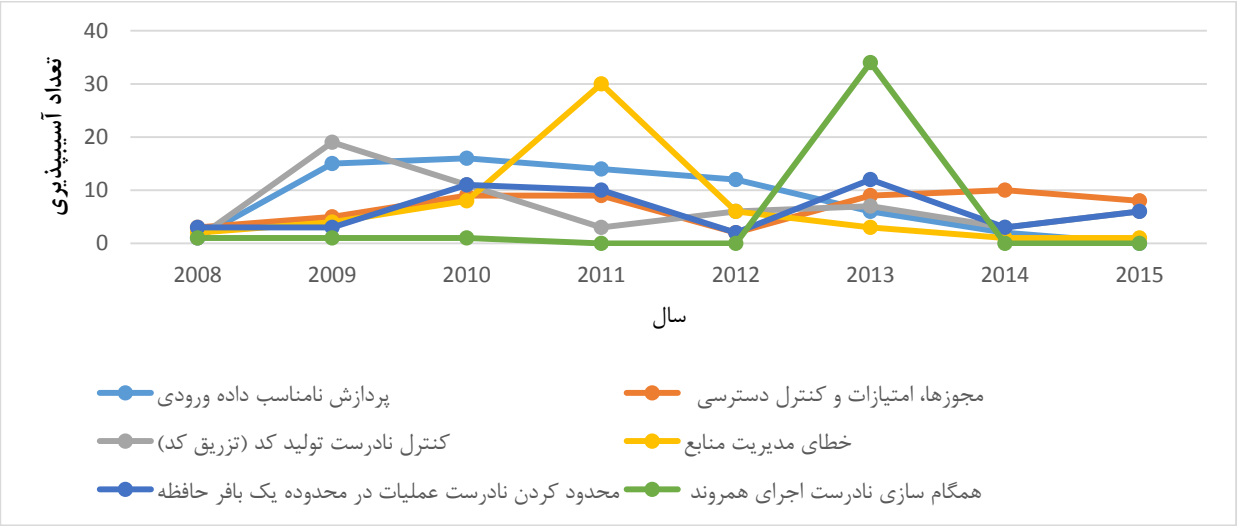


شکل ۳۰- انواع ضعف‌های ویندوز سرور ۲۰۰۳

جدول ۳۱ روند تغییر انواع ضعف‌ها در طول سال‌ها را نمایش می‌دهد. انواع ضعف‌های ویندوز ۲۰۰۳ در طول سال‌ها دچار تغییرات زیادی شده است. روند کلی کاهش تعداد انواع ضعف‌ها در طول سال‌ها قابل ملاحظه می‌باشد با توجه به تعداد کم آسیب‌پذیری‌ها در سال‌های اخیر، نمودار فقط تا سال ۲۰۱۹ رسم شده است. ضعف همگام‌سازی نادرست اجرای همروند که در طول سال‌ها بسیار کم بوده به صورت ناگهانی در سال ۲۰۱۳ در ۳۵ آسیب‌پذیری دیده می‌شود و مجددا روند رو به کاهش را طی می‌کند.

جدول ۳۱- روند تغییر انواع ضعف‌های ویندوز ۲۰۰۳

سال	پردازش نامناسب داده ورودی	مجوزها، امتیازات و کنترل دسترسی	کنترل نادرست تولید کد	خطای مدیریت منابع	محدود کردن نادرست عملیات در محدوده یک بافر حافظه	همگام سازی نادرست اجرای همروند
۲۰۰۶	۰	۱	۰	۰	۱	۰
۲۰۰۷	۰	۰	۰	۰	۰	۰
۲۰۰۸	۱	۳	۱	۲	۳	۱
۲۰۰۹	۱۵	۵	۱۹	۴	۳	۱
۲۰۱۰	۱۶	۹	۱۱	۸	۱۱	۱
۲۰۱۱	۱۴	۹	۳	۳۰	۱۰	۰
۲۰۱۲	۱۲	۲	۶	۶	۲	۰
۲۰۱۳	۶	۹	۷	۳	۱۲	۳۴
۲۰۱۴	۲	۱۰	۳	۱	۳	۰
۲۰۱۵	۰	۲۰۰	۶	۱	۶	۰

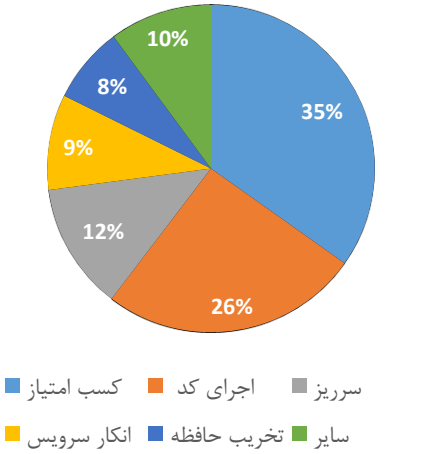


شکل ۳۱- روند تغییر انواع ضعف‌های ویندوز ۲۰۰۳

بر اساس اطلاعات جمع‌آوری شده آسیب‌پذیری از نوع "کسب امتیاز" ۳۳٪ از انواع آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۰۳ را تشکیل می‌دهد و بعد از آن اجرای کد و سرریز به ترتیب با ۲۶٪ و ۱۲٪ آسیب‌پذیری در رتبه دوم و سوم قرار دارند. در مقایسه انواع آسیب‌پذیری‌ها کشف شده در ویندوز سرورها با آسیب‌پذیری‌های ارائه شده برای ویندوز ۲۰۰۳، متوجه می‌شویم که نوع آسیب‌پذیری کسب اطلاعات در این سیستم‌عامل محدود است و در مقابل آسیب‌پذیری از نوع کسب امتیاز بسیار زیاد می‌باشد. دلیل کم بودن آسیب‌پذیری از نوع کسب اطلاعات در این ویندوز سرور تعداد کم آسیب‌پذیری‌ها با شدت پایین می‌باشد.

جدول ۳۲ - فراوانی انواع آسیب‌پذیری‌های ویندوز سرور ۲۰۰۳

نوع آسیب‌پذیری	تعداد آسیب‌پذیری
کسب امتیاز	۲۰۳
اجرای کد	۱۴۹
سرریز	۷۳
انکار سرویس	۵۵
تخریب حافظه	۴۴
بقیه	۵۹



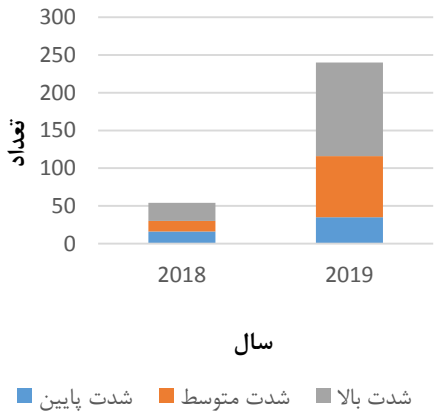
شکل ۳۲- انواع آسیب‌پذیری‌های ویندوز ۲۰۰۳

۳-۵- ویندوز سرور ۲۰۱۹

بر اساس داده‌های جدول ۳۳، گزارش آسیب‌پذیری برای ویندوز سرور ۲۰۱۹ از همان سال اولیه انتشار این سیستم‌عامل آغاز شد. در سال ۲۰۱۸ بیش از ۵۰ آسیب‌پذیری برای ویندوز ۲۰۱۹ منتشر شد که تقریبا نیمی از آن دارای شدت بالا بودند. تعداد آسیب‌پذیری‌های منتشر شده در سال ۲۰۱۹ به شدت افزایش یافت و ۲۴۰ آسیب‌پذیری در این سال منتشر شد که تقریبا بیش از ۵۰٪ از آن‌ها دارای شدت بالا بودند. تعداد زیاد آسیب‌پذیری‌های منتشر شده برای این سیستم‌عامل در سال جاری میلادی نشان از اهمیت رفع آسیب‌پذیری این ویندوز سرور جدید دارد.

جدول ۳۳- فراوانی شدت آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۱۹

	شدت آسیب‌پذیری		
	بالا	متوسط	پایین
۲۰۱۸	۲۴	۱۴	۱۶
۲۰۱۹	۱۲۴	۸۱	۳۵



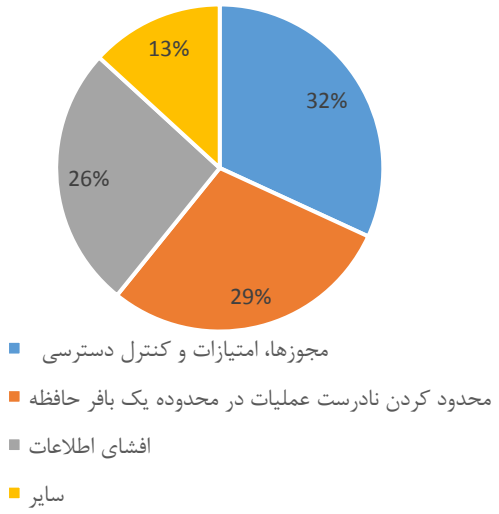
شکل ۳۳- فراوانی شدت آسیب‌پذیری‌های منتشر شده برای ویندوز

سرور ۲۰۱۹

با توجه به این‌که تعداد آسیب‌پذیری‌های منتشر شده برای ویندوز سرور ۲۰۱۹ بسیار محدود می‌باشد، نمی‌توان به صورت دقیق از انواع ضعف‌های آن بحث کرد. اما با بررسی آسیب‌پذیری‌هایی که تاکنون شناسایی شده‌اند، مهم‌ترین ضعف این ویندوز سرور سه نوع ضعف "مجوزها، امتیازات و کنترل دسترسی"، "محدود کردن نادرست عملیات در محدوده یک بافر حافظه" و افشای اطلاعات می‌باشد. این سه نوع ضعف ۸۷٪ از انواع ضعف‌های این سیستم‌عامل را تشکیل می‌دهند. در جدول ۳۴ فراوانی انواع ضعف‌های ویندوز سرور ۲۰۱۹ مشخص شده است.

جدول ۳۴- فراوانی انواع ضعف‌های ویندوز سرور ۲۰۱۹

نوع ضعف	تعداد آسیب‌پذیری
مجوزها، امتیازات و کنترل دسترسی	۸۷
محدود کردن نادرست عملیات در محدوده یک بافر حافظه	۷۹
افشای اطلاعات	۷۱
سایر	۳۶

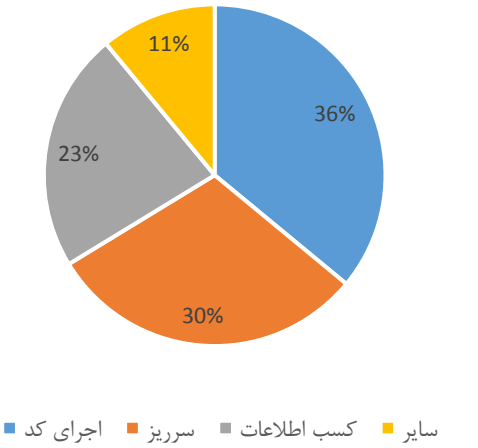


شکل ۳۴- انواع ضعف‌های ویندوز سرور ۲۰۱۹

بر اساس نتایج حاصل از بررسی‌های انجام شده، ۸۹٪ از انواع آسیب‌پذیری‌های ویندوز سرور ۲۰۱۹ به ترتیب از ۳۶٪ اجرای کد، ۳۰٪ سرریز و ۲۳٪ کسب اطلاعات تشکیل شده است. در این ویندوز سرور نیز بررسی تاثیر شدت آسیب‌پذیری‌ها بر روی نوع آسیب‌پذیری نشان از شدت پایین آسیب‌پذیری از نوع کسب اطلاعات دارد. شکل ۳۵ انواع آسیب‌پذیری‌های ویندوز سرور ۲۰۱۹ را نمایش می‌دهد.

جدول ۳۵- فراوانی انواع آسیب‌پذیری‌های ویندوز سرور ۲۰۱۹

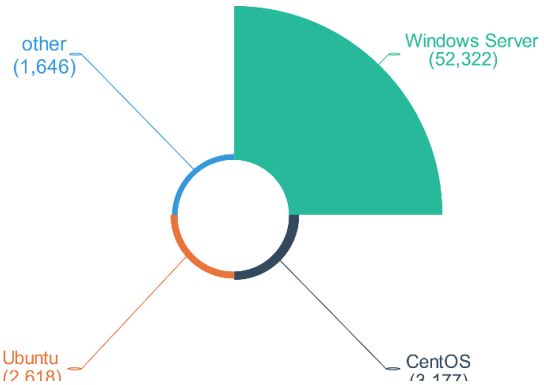
نوع آسیب‌پذیری	تعداد آسیب‌پذیری‌ها
اجرای کد	۹۵
سرریز	۸۰
کسب اطلاعات	۶۰
سایر	۲۹



شکل ۳۵- انواع آسیب‌پذیری‌های ویندوز سرور ۲۰۱۹

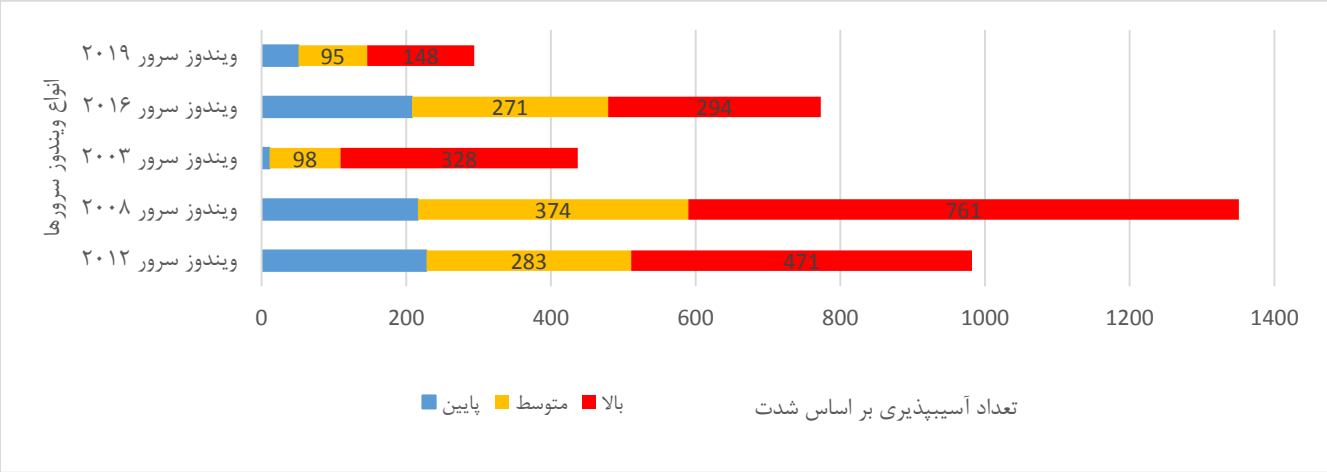
جمع بندی و نتیجه‌گیری

یکی از زیرساخت‌های اصلی در توسعه و راه‌اندازی سامانه‌های تحت وب، سیستم‌عامل‌ها می‌باشند که به عنوان پلتفرم زیرین جهت اجرای سرویس‌های دیگر مانند وب‌سرور و پایگاه‌داده مورد استفاده قرار می‌گیرند. در حال حاضر ۸۷٪ از سیستم‌عامل-های فضای وب کشور را که موفق به شناسایی نوع آن‌ها شده‌ایم؛ ویندوز سرورها تشکیل می‌دهند. با توجه به فراوانی استفاده از ویندوز سرورها در کشور، آسیب‌پذیرها و بدافزارهای منتشر شده برای ویندوز سرورها، بخش عمده‌ای از زیرساخت‌های کشور را تحت تاثیر قرار می‌دهد. از این رو برآن شدیم تا به بررسی آسیب‌پذیری‌های شناسایی شده برای ویندوز سرورها بپردازیم.



شکل ۳۶- فراوانی انواع سیستم‌عامل‌های شناسایی شده

با توجه به ارزیابی‌های انجام شده ۳۷٪ از ویندوز سرورهای شناسایی شده را ویندوز سرور 2012 R2 تشکیل می‌دهد که در حدود ۱۰۰۰ آسیب‌پذیری برای آن منتشر شده است. اجرای کد و کسب امتیاز دو آسیب‌پذیری هستند که بیشترین تاثیر را بر روی این ویندوز سرور دارند. ویندوز سرور 2008 R2 با ۲۴٪ در رتبه دوم ویندوز سرورهای پر طرفدار در کشور قرار دارد. برای این ویندوز سرور حدود ۱۴۰۰ آسیب‌پذیری منتشر شده است که ناشی از دو نوع "ضعف مجوزها، امتیازات و کنترل دسترسی" و افشای اطلاعات می‌باشند. نکته نگران‌کننده در مورد این ویندوز سرور این است که از سال ۲۰۲۰ از این سیستم‌عامل پشتیبانی نخواهد شد و بروزرسانی برای آن ارائه نمی‌شود. یکی دیگر از ویندوز سرورهای که از آن توصیه نمی-شود، ویندوز سرور ۲۰۰۳ می‌باشد. مایکروسافت پشتیبانی از این ویندوز سرور را در سال ۲۰۱۵ متوقف کرده است و برای این محصول بروزرسانی تولید نمی‌کند. با این وجود هنوز هم ۳٪ از ویندوز سرورهای استفاده شده در کشور از این محصول استفاده می‌کنند.



شکل ۳۷- فراوانی آسیب‌پذیری‌های منتشر شده برای ویندوز سرورهای مختلف

CVEها به صورت عمومی منتشر می‌شوند و در اختیار هکرها نیز قرار دارند. یکی از خطرناک‌ترین نمونه‌های آسیب‌پذیری‌ها CVE-2017-0144 بود که به صورت گسترده توسط هکرها مورد سوء استفاده واقع شد و توسط باج‌افزار Wannacrypt مورد بهره‌برداری قرار گرفت. بنابراین ضروری است تا در اسرع وقت بروزرسانی‌های لازم برای هر آسیب‌پذیری انجام شود. در ضمیمه ۱ بروزرسانی‌ها مرتبط با آسیب‌پذیری‌ها دارای شدت بالا ارائه شده تا خوانندگان این سند بتوانند امنیت سیستم خود را تامین نمایند.

آسیب‌پذیری‌های بررسی شده در این سند تا تاریخ ۱۳۹۸/۰۵/۰۶می‌باشد. باور بر این بوده است که اطلاعات استفاده شده از منابع ذکر شده قابل اطمینان می‌باشند، اما به هیچ وجه تضمین شده نخواهد بود.