بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

رفع ۱۲۹ آسیب‌پذیری در اصلاحیه سپتامبر مایکروسافت سال ۲۰۲۰ میلادی

خبر آسیب‌پذیری

شناسه سند ..... Maher_13990620….

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۳۹۹/۰۶/۱۹

طبقه‌بندی سند ..... **عادی**

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰

(۰۲۱) ۴۲۶۵۰۰۰۰

cert.ir

فهرست مطالب

۱ رفع ۱۲۹ آسیب‌پذیری در اصلاحیه سپتامبر مایکروسافت سال ۲۰۲۰ میلادی

مایکروسافت در اصلاحیه‌ای که ۸ سپتامبر ۲۰۲۰ میلادی منتشر کرد برای ۱۲۹ آسیب‌پذیری محصولات خود، وصله ارائه نموده‌است. از میان این آسیب‌پذیری‌ها ۲۳ مورد جزء دسته‌بندی آسیب‌پذیرها با درجه اهمیت بحرانی (Critical) هستند، ۱۰۵ مورد در دسته‌بندی با درجه اهمیت مهم (Important) قرار دارند و یک مورد نیز در دسته‌بندی با درجه اهمیت متوسط (Moderate) قرار دارد.

خوشبختانه هیچ آسیب‌پذیری روز صفری در میان آسیب‌پذیری‌های رفع شده در اصلاحیه سپتامبر وجود ندارد. با این وجود، چند آسیب‌پذیری با درجه اهمیت بحرانی که منجر به اجرای کد از راه دور می‌شوند، در این اصلاحیه رفع شده است. سه مورد جالب توجه از این آسیب‌پذیری عبارتند از:

- آسیب‌پذیری بروز اختلال در حافظه در Microsoft Exchange که دارای شناسه CVE-2020-16875 است به مهاجمان راه دور این امکان را می‌دهد که با ارسال ایمیل جعلی به سرور Exchange server، اجرای کد از راه دور انجام دهند.
- آسیب‌پذیری در مولفه Microsoft Component Object Model (COM) ویندوز که دارای شناسه CVE-2020-0922 است، این امکان را به مهاجم راه دور احراز هویت نشده می‌دهد تا با اغوای کاربر و هدایت وی به سایت با جاوااسکریپ مخرب کد مورد نظر خود را از راه دور در سیستم کاربر اجرا نماید.
- آسیب‌پذیری در مولفه Text Service Module ویندوز که دارای شناسه CVE-2020-0908 است، موجب اجرای کد از راه دور در این سیستم‌عامل می‌شود. بهره‌برداری از این آسیب‌پذیری با ترغیب کاربر برای مشاهده سایت دارای محتوای آسیب‌پذیر انجام می‌شود.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های این ماه مایکروسافت در جدول زیر ارائه شده است:

محصول	شناسه CVE	نوع آسیب‌پذیری	درجه اهمیت
Active Directory	CVE-2020-0761	اجرای کد از راه دور (Remote Code Execution)	مهم
Active Directory	CVE-2020-0856	افشای اطلاعات (Information Disclosure)	مهم
Active Directory	CVE-2020-0718	اجرای کد از راه دور	مهم

Active Directory	CVE-2020-0664	افشای اطلاعات	مهم
Active Directory Federation Services	CVE-2020-0837	Spoofing Vulnerability	مهم
ASP.NET	CVE-2020-1045	Feature Bypass	مهم
Common Log File System Driver	CVE-2020-1115	ترفیع امتیازی (Elevation of Privilege)	مهم
Internet Explorer	CVE-2020-1012	ترفیع امتیازی	مهم
Internet Explorer	CVE-2020-16884	بروز اختلال در حافظه (Memory Corruption)	مهم
Internet Explorer	CVE-2020-1506	ترفیع امتیازی	مهم
Microsoft Browsers	CVE-2020-0878	ترفیع امتیازی	بحرانی
Microsoft Dynamics	CVE-2020-16857	اجرای کد از راه دور	بحرانی
Microsoft Dynamics	CVE-2020-16858	تزریق اسکریپت (XSS)	مهم
Microsoft Dynamics	CVE-2020-16860	اجرای کد از راه دور	مهم
Microsoft Dynamics	CVE-2020-16859	تزریق اسکریپت (XSS)	مهم
Microsoft Dynamics	CVE-2020-16861	تزریق اسکریپت (XSS)	مهم
Microsoft Dynamics	CVE-2020-16872	تزریق اسکریپت (XSS)	مهم
Microsoft Dynamics	CVE-2020-16864	تزریق اسکریپت (XSS)	مهم
Microsoft Dynamics	CVE-2020-16878	تزریق اسکریپت (XSS)	مهم
Microsoft Dynamics	CVE-2020-16862	اجرای کد از راه دور	بحرانی
Microsoft Dynamics	CVE-2020-16871	تزریق اسکریپت (XSS)	مهم
Microsoft Exchange Server	CVE-2020-16875	بروز اختلال در حافظه	بحرانی

Microsoft Graphics Component	CVE-2020-0921	افشای اطلاعات	مهم
Microsoft Graphics Component	CVE-2020-0998	ترفیع امتیازی	مهم
Microsoft Graphics Component	CVE-2020-1091	افشای اطلاعات	مهم
Microsoft Graphics Component	CVE-2020-1152	ترفیع امتیازی	مهم
Microsoft Graphics Component	CVE-2020-1097	افشای اطلاعات	مهم
Microsoft Graphics Component	CVE-2020-1083	افشای اطلاعات	مهم
Microsoft Graphics Component	CVE-2020-1053	ترفیع امتیازی	مهم
Microsoft Graphics Component	CVE-2020-1308	ترفیع امتیازی	مهم
Microsoft Graphics Component	CVE-2020-1245	ترفیع امتیازی	مهم
Microsoft Graphics Component	CVE-2020-1285	اجرای کد از راه دور	بحرانی
Microsoft Graphics Component	CVE-2020-1256	افشای اطلاعات	مهم
Microsoft Graphics Component	CVE-2020-1250	افشای اطلاعات	مهم
Microsoft JET Database Engine	CVE-2020-1039	اجرای کد از راه دور	مهم
Microsoft JET Database Engine	CVE-2020-1074	اجرای کد از راه دور	مهم
Microsoft NTFS	CVE-2020-0838	ترفیع امتیازی	مهم
Microsoft Office	CVE-2020-1594	اجرای کد از راه دور	مهم
Microsoft Office	CVE-2020-1335	اجرای کد از راه دور	مهم
Microsoft Office	CVE-2020-16855	افشای اطلاعات	مهم
Microsoft Office	CVE-2020-1338	اجرای کد از راه دور	مهم
Microsoft Office	CVE-2020-1332	اجرای کد از راه دور	مهم

Microsoft Office	CVE-2020-1224	افشای اطلاعات	مهم
Microsoft Office	CVE-2020-1218	اجرای کد از راه دور	مهم
Microsoft Office	CVE-2020-1193	اجرای کد از راه دور	مهم
Microsoft Office SharePoint	CVE-2020-1345	تزریق اسکریپت (XSS)	مهم
Microsoft Office SharePoint	CVE-2020-1205	Spoofing	مهم
Microsoft Office SharePoint	CVE-2020-1210	اجرای کد از راه دور	بحرانی
Microsoft Office SharePoint	CVE-2020-1514	تزریق اسکریپت (XSS)	مهم
Microsoft Office SharePoint	CVE-2020-1595	اجرای کد از راه دور	بحرانی
Microsoft Office SharePoint	CVE-2020-1523	Tampering Vulnerability	مهم
Microsoft Office SharePoint	CVE-2020-1440	Tampering Vulnerability	مهم
Microsoft Office SharePoint	CVE-2020-1200	اجرای کد از راه دور	بحرانی
Microsoft Office SharePoint	CVE-2020-1482	تزریق اسکریپت (XSS)	مهم
Microsoft Office SharePoint	CVE-2020-1198	تزریق اسکریپت (XSS)	مهم
Microsoft Office SharePoint	CVE-2020-1227	تزریق اسکریپت (XSS)	مهم
Microsoft Office SharePoint	CVE-2020-1576	اجرای کد از راه دور	بحرانی
Microsoft Office SharePoint	CVE-2020-1452	اجرای کد از راه دور	بحرانی
Microsoft Office SharePoint	CVE-2020-1575	تزریق اسکریپت (XSS)	مهم
Microsoft Office SharePoint	CVE-2020-1453	اجرای کد از راه دور	بحرانی
Microsoft Office SharePoint	CVE-2020-1460	اجرای کد از راه دور	بحرانی

Microsoft OneDrive	CVE-2020-16853	ترفیع امتیازی	مهم
Microsoft OneDrive	CVE-2020-16851	ترفیع امتیازی	مهم
Microsoft OneDrive	CVE-2020-16852	افشای اطلاعات	مهم
Microsoft Scripting Engine	CVE-2020-1057	بروز اختلال در حافظه	بحرانی
Microsoft Scripting Engine	CVE-2020-1180	بروز اختلال در حافظه	مهم
Microsoft Scripting Engine	CVE-2020-1172	بروز اختلال در حافظه	بحرانی
Microsoft Windows	CVE-2020-1596	افشای اطلاعات	مهم
Microsoft Windows	CVE-2020-1169	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1593	اجرای کد از راه دور	بحرانی
Microsoft Windows	CVE-2020-1159	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1598	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-0790	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-0922	اجرای کد از راه دور	بحرانی
Microsoft Windows	CVE-2020-0782	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-0648	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-0766	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1590	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1376	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1471	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-16879	افشای اطلاعات	مهم
Microsoft Windows	CVE-2020-1013	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1532	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1491	ترفیع امتیازی	مهم

Microsoft Windows	CVE-2020-1303	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1252	اجرای کد از راه دور	بحرانی
Microsoft Windows	CVE-2020-1559	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1507	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1508	اجرای کد از راه دور	بحرانی
Microsoft Windows	CVE-2020-0914	افشای اطلاعات	مهم
Microsoft Windows	CVE-2020-0886	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-0989	افشای اطلاعات	مهم
Microsoft Windows	CVE-2020-0875	افشای اطلاعات	مهم
Microsoft Windows	CVE-2020-0912	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1038	انکار سرویس (Denial of Service)	مهم
Microsoft Windows	CVE-2020-0908	اجرای کد از راه دور	بحرانی
Microsoft Windows	CVE-2020-1052	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-0911	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-0805	دور زدن ویژگی امنیتی	مهم
Microsoft Windows	CVE-2020-1119	افشای اطلاعات	مهم
Microsoft Windows	CVE-2020-1146	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-0951	دور زدن ویژگی امنیتی (Security Feature Bypass)	مهم
Microsoft Windows	CVE-2020-1122	ترفیع امتیازی	مهم
Microsoft Windows	CVE-2020-1098	ترفیع امتیازی	مهم
Microsoft Windows Codecs Library	CVE-2020-1319	کد از راه دور	بحرانی

Microsoft Windows Codecs Library	CVE-2020-0997	اجرای کد از راه دور	بحرانی
Microsoft Windows Codecs Library	CVE-2020-1129	اجرای کد از راه دور	بحرانی
Microsoft Windows DNS	CVE-2020-0839	ترفیع امتیازی	مهم
Microsoft Windows DNS	CVE-2020-1228	انکار سرویس (Denial of Service)	مهم
Microsoft Windows DNS	CVE-2020-0836	انکار سرویس	مهم
Open Source Software	CVE-2020-16873	Spoofing Vulnerability	مهم
SQL Server	CVE-2020-1044	دور زدن ویژگی امنیتی	متوسط
Visual Studio	CVE-2020-16874	اجرای کد از راه دور	بحرانی
Visual Studio	CVE-2020-16856	اجرای کد از راه دور	مهم
Visual Studio	CVE-2020-16881	اجرای کد از راه دور	مهم
Windows DHCP Server	CVE-2020-1031	افشای اطلاعات	مهم
Windows Diagnostic Hub	CVE-2020-1130	ترفیع امتیازی	مهم
Windows Diagnostic Hub	CVE-2020-1133	ترفیع امتیازی	مهم
Windows Hyper-V	CVE-2020-0904	انکار سرویس	مهم
Windows Hyper-V	CVE-2020-0890	انکار سرویس	مهم
Windows Kernel	CVE-2020-0941	افشای اطلاعات	مهم
Windows Kernel	CVE-2020-0928	افشای اطلاعات	مهم
Windows Kernel	CVE-2020-16854	افشای اطلاعات	مهم
Windows Kernel	CVE-2020-1034	ترفیع امتیازی	مهم
Windows Kernel	CVE-2020-1033	افشای اطلاعات	مهم
Windows Kernel	CVE-2020-1589	افشای اطلاعات	مهم

Windows Kernel	CVE-2020-1592	افشای اطلاعات	مهم
Windows Print Spooler Components	CVE-2020-1030	ترفیع امتیازی	مهم
Windows Shell	CVE-2020-0870	ترفیع امتیازی	مهم

منابع

[1] https://www.zdnet.com/article/microsoft-september-2020-patch-tuesday-fixes-129-vulnerabilities/

[2] https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2020-patch-tuesday-fixes-129-vulnerabilities/