

بسمه تعالی



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

رفع ۵۸ آسیب پذیری توسط مایکروسافت در ماه دسامبر

آسیب پذیری

شناسه سند MaherReport_13990920-01
نوع سند گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۰۹/۲۰
طبقه بندی سند **عادی**

تهران، خیابان شهید بهشتی، نرسیده به قائم مقام فراهانی، پلاک ۲۶۷، سازمان فناوری اطلاعات ایران



cert.ir

۰۲۱) ۴۲۶۵۰۰۰۰



۰۲۱) ۴۲۶۵۰۰۰۰





رفع ۵۸ آسیب پذیری توسط میکروسافت در ماه دسامبر ۱

۱ رفع ۵۸ آسیب پذیری توسط مایکروسافت در ماه دسامبر

به روزرسانی امنیتی ماه دسامبر مایکروسافت شامل وصله‌هایی برای رفع ۵۸ آسیب‌پذیری در محصولات مختلف این شرکت و یک توصیه امنیتی است. از میان ۵۸ آسیب‌پذیری رفع شده در به روزرسانی امنیتی اخیر مایکروسافت، ۹ مورد جزء آسیب‌پذیری‌های بحرانی، ۴۸ مورد جزء آسیب‌پذیری‌های مهم و دو مورد جزء آسیب‌پذیری‌های متوسط دسته‌بندی شده‌اند.

خوشبختانه آسیب‌پذیری روز صفر یا آسیب‌پذیری که قبلاً افشاء شده باشد در میان آسیب‌پذیری‌های رفع شده وجود ندارد. چند مورد از آسیب‌پذیری‌های قابل توجه رفع شده در این به‌روزرسانی به شرح زیر است.

- آسیب‌پذیری با شناسه CVE-2020-17095: این آسیب‌پذیری به برنامه‌های مخرب اجرا شده در Hyper-V VM اجازه اجرای کد در هاست را می‌دهد.
- آسیب‌پذیری با شناسه CVE-2020-17096: آسیب‌پذیری NTFS ویندوز می‌تواند به صورت محلی برای افزایش مجوزها یا از راه دور از طریق SMBv2 برای اجرای دستورات مورد سو استفاده قرار بگیرد.
- آسیب‌پذیری با شناسه CVE-2020-17099: این آسیب‌پذیری موجب دور زدن ویژگی امنیتی Lock Screen در ویندوز شده و امکان اجرای دستورات را برای کاربر لوکال در حالتی که دستگاه ویندوز قفل است، فراهم می‌آورد.

مایکروسافت یک توصیه برای رفع آسیب‌پذیری DNS cache poisoning منتشر کرده است. اکسپلویت موفق این آسیب‌پذیری به مهاجمان این امکان را می‌دهد تا از رکوردهای DNS دستکاری شده برای انتقال کاربران به وبسایت‌های مخرب تحت کنترل مهاجمان استفاده کنند.

این آسیب‌پذیری که با شناسه CVE-2020-25705 پیگیری می‌شود در مولفه نرم افزاری Windows DNS Resolver software وجود دارد. برای رفع این آسیب‌پذیری، مدیران باید Registry را تغییر دهند و حداکثر سایز بسته‌های UDP را برابر 1,221 قرار دهند. برای بسته‌های بزرگتر از این سایز DNS resolver به ارتباط TCP سوئیچ خواهد کرد.

جدول ۱ لیست آسیب‌پذیری‌های رفع شده در این به‌روزرسانی امنیتی را نمایش می‌دهد.

جدول ۱- لیست آسیب پذیری های منتشر شده در به روزرسانی ماه دسامبر

نام محصول	شدت آسیب پذیری	شناسه آسیب پذیری
Azure DevOps	مهم	CVE-2020-17145
Azure DevOps	مهم	CVE-2020-17135
Azure SDK	مهم	CVE-2020-17002
Azure SDK	مهم	CVE-2020-16971
Azure Sphere	مهم	CVE-2020-17160
Microsoft Dynamics	مهم	CVE-2020-17147
Microsoft Dynamics	مهم	CVE-2020-17133
Microsoft Dynamics	بحرانی	CVE-2020-17158
Microsoft Dynamics	بحرانی	CVE-2020-17152
Microsoft Edge	متوسط	CVE-2020-17153
Microsoft Edge	بحرانی	CVE-2020-17131
Microsoft Exchange Server	مهم	CVE-2020-17143
Microsoft Exchange Server	مهم	CVE-2020-17144
Microsoft Exchange Server	مهم	CVE-2020-17141
Microsoft Exchange Server	بحرانی	CVE-2020-17117
Microsoft Exchange Server	بحرانی	CVE-2020-17132
Microsoft Exchange Server	بحرانی	CVE-2020-17142
Microsoft Graphics Component	مهم	CVE-2020-17137
Microsoft Graphics Component	مهم	CVE-2020-17098
Microsoft Office	مهم	CVE-2020-17130
Microsoft Office	مهم	CVE-2020-17128

Microsoft Office	مهم	CVE-2020-17129
Microsoft Office	مهم	CVE-2020-17124
Microsoft Office	مهم	CVE-2020-17123
Microsoft Office	مهم	CVE-2020-17119
Microsoft Office	مهم	CVE-2020-17125
Microsoft Office	مهم	CVE-2020-17127
Microsoft Office	مهم	CVE-2020-17126
Microsoft Office	مهم	CVE-2020-17122
Microsoft Office SharePoint	متوسط	CVE-2020-17115
Microsoft Office SharePoint	مهم	CVE-2020-17120
Microsoft Office SharePoint	بحرانی	CVE-2020-17121
Microsoft Office SharePoint	بحرانی	CVE-2020-17118
Microsoft Office SharePoint	مهم	CVE-2020-17089
Microsoft Windows	مهم	CVE-2020-17136
Microsoft Windows	مهم	CVE-2020-16996
Microsoft Windows	مهم	CVE-2020-17138
Microsoft Windows	مهم	CVE-2020-17092
Microsoft Windows	مهم	CVE-2020-17139
Microsoft Windows	مهم	CVE-2020-17103
Microsoft Windows	مهم	CVE-2020-17134
Microsoft Windows DNS	مهم	ADV200013
Visual Studio	مهم	CVE-2020-17148
Visual Studio	مهم	CVE-2020-17159

Visual Studio	مهم	CVE-2020-17156
Visual Studio	مهم	CVE-2020-17150
Windows Backup Engine	مهم	CVE-2020-16960
Windows Backup Engine	مهم	CVE-2020-16958
Windows Backup Engine	مهم	CVE-2020-16959
Windows Backup Engine	مهم	CVE-2020-16961
Windows Backup Engine	مهم	CVE-2020-16964
Windows Backup Engine	مهم	CVE-2020-16963
Windows Backup Engine	مهم	CVE-2020-16962
Windows Error Reporting	مهم	CVE-2020-17094
Windows Hyper-V	بحرانی	CVE-2020-17095
Windows Lock Screen	مهم	CVE-2020-17099
Windows Media	مهم	CVE-2020-17097
Windows SMB	مهم	CVE-2020-17096
Windows SMB	مهم	CVE-2020-17140

منبع

<https://www.zdnet.com/article/microsoft-december-2020-patch-tuesday-fixes-58-vulnerabilities/>