بسمه تعالی

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

بروزرسانی محصولات مایکروسافت آگوست

خبر آسیب‌پذیری

شناسه سند ..... Maher_1399052601
نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۰۵/۲۶
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 مقدمه

مایکروسافت به تازگی مجموعه‌ای از به‌روزرسانی‌ها را برای ۱۳ محصول مختلف خود منتشر کرده است که ۱۲۰ آسیب‌پذیری را در این محصولات رفع می‌کند. ۱۷ مورد از این آسیب‌پذیری‌ها بحرانی هستند و دو مورد از آن‌ها، آسیب‌پذیری روز صفرم می‌باشند که قبل از انتشار این به‌روزرسانی توسط هکرها بهره‌برداری شده‌اند.

۲ محصولات تحت تاثیر آسیب‌پذیری

به‌روزرسانی منتشر شده در ۱۱ اگوست برای ۱۳ نرم‌افزار وصله امنیتی ارائه شده است:

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based)
- Microsoft ChakraCore
- Internet Explorer
- Microsoft Scripting Engine
- SQL Server
- Microsoft JET Database Engine
- .NET Framework
- ASP.NET Core
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Microsoft Dynamics

کاربران گرامی برای آگاهی از نسخه‌های نیازمند به‌روزرسانی و نحوه‌ی انجام به‌روزرسانی می‌توانید از سایت مایکروسافت استفاده نمایید. همچنین فایل ضمیمه با نام "Affected_product.xlsx" شامل لیست تمام محصولات تحت تاثیر، مقاله KB مرتبط و آدرس فایل دانلود بروزرسانی همه نسخه‌های نیازمند به‌روزرسانی می‌باشد.

کاربران سیستم‌عامل ویندوز لازم است توجه نمایند، چنانکه از هر یک از نسخه‌های پشتیبانی شده سیستم‌عامل ویندوز ۳۲ بیتی یا ۶۴ بیتی استفاده می‌کنید. سیستم‌عامل شما نیازمند به‌روزرسانی می‌باشد.

۳ آسیب‌پذیری‌های روز صفرم

دو آسیب‌پذیری روز صفرم با شناسه‌های CVE-2020-1464 و CVE-2020-1380 قبل از انتشار وصله در ۱۱ اگوست توسط هکرها مورد بهره‌برداری قرارگرفته‌است.

۳-۱ آسیب‌پذیری CVE-2020-1464

باگ سیستم‌عامل ویندوز که با شناسه CVE-2020-1464 شناخته می‌شود؛ موجب اعتبارسنجی نادرست امضاء فایل می‌شود. بنابراین هکرها با بهره‌برداری از این باگ می‌توانند ویژگی‌های امنیتی را دور زده و فایل‌هایی با امضای نادرست را لود کنند.

۳-۲ آسیب‌پذیری CVE-2020-1380

آسیب‌پذیری با شناسه CVE-2020-1380 ناشی از باگی در موتور اسکریپت مرورگر Internet Explorer است. با وجود اینکه آسیب‌پذیری در موتور اسکریپت مرورگر IE است، دیگر محصولات مایکروسافت مانند مجموعه Office نیز تحت تاثیر این آسیب‌پذیری قرار دارند. دلیل این اتفاق استفاده برنامه‌های Office از موتور اسکریپت مرورگر IE برای تعبیه و render صفحات وب در داکیومنت‌های Office است.

براساس گزارش‌های کسپرسکی نفوذگران با بهره‌برداری از آسیب‌پذیری مذکور و آسیب‌پذیری ترفیع امتیاز ویندوز ۱۰ (آسیب‌پذیری با شناسه CVE-2020-0986) به شرکت‌های کره‌جنوبی حمله کرده‌اند. کسپرسکی بیان کرده‌است که شرکت‌ها با استقرار Virtual Area Networks می‌توانند از داده‌های خود محافظت نمایند. همچنین استفاده از فایروال در سیستم وایفا برای محافظت از بدافزارهای wirless ضروری است. کاربران معمولی نیز می‌توانند با بروزرسانی مرورگر IE و ویندوز ۱۰و عدم استفاده از وب‌سایت‌های بدون گواهی SSL از خود در برابر این آسیب‌پذیری محافظت کنند.

۴ لیست آسیب‌پذیری‌های

در جدول آسیب‌پذیری‌ها رفع شده در به‌روزرسانی ماه اگوست ۲۰۲۰ نمایش داده‌شده‌است.

محصول	شناسه آسیب‌پذیری	شدت آسیب‌پذیری
.NET Framework	CVE-2020-1476	مهم
.NET Framework	CVE-2020-1046	بحرانی
ASP.NET	CVE-2020-1597	مهم
Internet Explorer	CVE-2020-1567	بحرانی
Microsoft Dynamics	CVE-2020-1591	مهم
Microsoft Edge	CVE-2020-1569	مهم
Microsoft Edge	CVE-2020-1568	بحرانی
Microsoft Graphics Component	CVE-2020-1562	مهم
Microsoft Graphics Component	CVE-2020-1577	مهم
Microsoft Graphics Component	CVE-2020-1561	مهم
Microsoft Graphics Component	CVE-2020-1510	مهم
Microsoft Graphics Component	CVE-2020-1529	مهم
Microsoft JET Database Engine	CVE-2020-1473	مهم
Microsoft JET Database Engine	CVE-2020-1558	مهم
Microsoft JET Database Engine	CVE-2020-1557	مهم
Microsoft JET Database Engine	CVE-2020-1564	مهم
Microsoft Office	CVE-2020-1483	بحرانی
Microsoft Office	CVE-2020-1504	مهم
Microsoft Office	CVE-2020-1503	مهم
Microsoft Office	CVE-2020-1495	مهم
Microsoft Office	CVE-2020-1494	مهم

Microsoft Office	CVE-2020-1493	مهم
Microsoft Office	CVE-2020-1496	مهم
Microsoft Office	CVE-2020-1502	مهم
Microsoft Office	CVE-2020-1498	مهم
Microsoft Office	CVE-2020-1497	مهم
Microsoft Office	CVE-2020-1581	مهم
Microsoft Office	CVE-2020-1563	مهم
Microsoft Office	CVE-2020-1582	مهم
Microsoft Office	CVE-2020-1583	مهم
Microsoft Office SharePoint	CVE-2020-1505	مهم
Microsoft Office SharePoint	CVE-2020-1573	مهم
Microsoft Office SharePoint	CVE-2020-1499	مهم
Microsoft Office SharePoint	CVE-2020-1500	مهم
Microsoft Office SharePoint	CVE-2020-1580	مهم
Microsoft Office SharePoint	CVE-2020-1501	مهم
Microsoft Scripting Engine	CVE-2020-1570	بحرانی
Microsoft Scripting Engine	CVE-2020-1555	بحرانی
Microsoft Scripting Engine	CVE-2020-1380	بحرانی
Microsoft Video Control	CVE-2020-1492	بحرانی
Microsoft Windows	CVE-2020-1485	مهم
Microsoft Windows	CVE-2020-1587	مهم
Microsoft Windows	CVE-2020-1551	مهم
Microsoft Windows	CVE-2020-1484	مهم

Microsoft Windows	CVE-2020-1489	مهم
Microsoft Windows	CVE-2020-1584	مهم
Microsoft Windows	CVE-2020-1486	مهم
Microsoft Windows	CVE-2020-1488	مهم
Microsoft Windows	CVE-2020-1490	مهم
Microsoft Windows	CVE-2020-1515	مهم
Microsoft Windows	CVE-2020-1513	مهم
Microsoft Windows	CVE-2020-1553	مهم
Microsoft Windows	CVE-2020-1552	مهم
Microsoft Windows	CVE-2020-1566	مهم
Microsoft Windows	CVE-2020-1579	مهم
Microsoft Windows	CVE-2020-1512	مهم
Microsoft Windows	CVE-2020-1511	مهم
Microsoft Windows	CVE-2020-1480	مهم
Microsoft Windows	CVE-2020-1542	مهم
Microsoft Windows	CVE-2020-1543	مهم
Microsoft Windows	CVE-2020-1540	مهم
Microsoft Windows	CVE-2020-1541	مهم
Microsoft Windows	CVE-2020-1544	مهم
Microsoft Windows	CVE-2020-1547	مهم
Microsoft Windows	CVE-2020-1519	مهم
Microsoft Windows	CVE-2020-1545	مهم
Microsoft Windows	CVE-2020-1546	مهم

Microsoft Windows	CVE-2020-1539	مهم
Microsoft Windows	CVE-2020-1528	مهم
Microsoft Windows	CVE-2020-1530	مهم
Microsoft Windows	CVE-2020-1526	مهم
Microsoft Windows	CVE-2020-1527	مهم
Microsoft Windows	CVE-2020-1534	مهم
Microsoft Windows	CVE-2020-1537	مهم
Microsoft Windows	CVE-2020-1520	مهم
Microsoft Windows	CVE-2020-1535	مهم
Microsoft Windows	CVE-2020-1536	مهم
Microsoft Windows	CVE-2020-1470	مهم
Microsoft Windows	CVE-2020-1509	مهم
Microsoft Windows	CVE-2020-1459	مهم
Microsoft Windows	CVE-2020-1538	مهم
Microsoft Windows	CVE-2020-1475	مهم
Microsoft Windows	CVE-2020-1464	مهم
Microsoft Windows	CVE-2020-1467	مهم
Microsoft Windows	CVE-2020-1550	مهم
Microsoft Windows	CVE-2020-1517	مهم
Microsoft Windows	CVE-2020-1518	مهم
Microsoft Windows	CVE-2020-1516	مهم
Microsoft Windows	CVE-2020-1549	مهم
Microsoft Windows	CVE-2020-1383	مهم

Microsoft Windows Codecs Library	CVE-2020-1574	بحرانی
Microsoft Windows Codecs Library	CVE-2020-1560	بحرانی
Microsoft Windows Codecs Library	CVE-2020-1585	بحرانی
Netlogon	CVE-2020-1472	بحرانی
SQL Server	CVE-2020-1455	مهم
Visual Studio	CVE-2020-0604	مهم
Windows AI	CVE-2020-1521	مهم
Windows AI	CVE-2020-1522	مهم
Windows AI	CVE-2020-1524	مهم
Windows COM	CVE-2020-1474	مهم
Windows Kernel	CVE-2020-1578	مهم
Windows Kernel	CVE-2020-1417	مهم
Windows Kernel	CVE-2020-1479	مهم
Windows Media	CVE-2020-1379	بحرانی
Windows Media	CVE-2020-1554	بحرانی
Windows Media	CVE-2020-1339	بحرانی
Windows Media	CVE-2020-1525	بحرانی
Windows Media	CVE-2020-1487	مهم
Windows Media Player	CVE-2020-1478	مهم
Windows Media Player	CVE-2020-1477	بحرانی
Windows Print Spooler Components	CVE-2020-1337	مهم
Windows RDP	CVE-2020-1466	مهم

Windows Registry	CVE-2020-1377	مهم
Windows Registry	CVE-2020-1378	مهم
Windows Shell	CVE-2020-1565	مهم
Windows Shell	CVE-2020-1531	مهم
Windows Update Stack	CVE-2020-1571	مهم
Windows Update Stack	CVE-2020-1548	مهم
Windows WalletService	CVE-2020-1556	مهم
Windows WalletService	CVE-2020-1533	مهم

منبع:

https://www.zdnet.com/article/microsoft-august-2020-patch-tuesday-fixes-120-vulnerabilities-two-zero-days/
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Aug
https://www.cybersecurity-insiders.com/zero-day-vulnerability-in-windows-os-and-internet-explorer-exploited/