VULNERABILITY BULLETINS

Microsoft Patches Six Zero-Day Security Holes

TLP:WHITE

Jun 09, 2021

As Microsoft has released over 50 security fixes in their recent
June Patch Tuesday for software to resolve critical and important issues,

Microsoft also mitigated six zero-days that are being actively exploited in the wild.

Additionally, please look forward to the monthly Heath-ISAC and Microsoft Patch Tuesday Podcast: Episode 4, where additional information discussing the related zero days will continue. You can access the new episode via Cyware, and access all past episodes.

Analysis:

The six zero-days that were patched by Microsoft are listed below:

- CVE-2021-33742, a remote code execution bug in a Windows HTML component.
- CVE-2021-31955, an information disclosure bug in the Windows Kernel
- CVE-2021-31956, an elevation of privilege flaw in Windows NTFS
- CVE-2021-33739, an elevation of privilege flaw in the Microsoft Desktop Window Manager
- CVE-2021-31201, an elevation of privilege flaw in the Microsoft Enhanced Cryptographic Provider
- CVE-2021-31199, an elevation of privilege flaw in the Microsoft Enhanced Cryptographic Provider

Flaws CVE-2021-31201 and CVE-2021-31199 are related to a patch Adobe released recently for CVE-2021-28550, a flaw in Adobe Acrobat and Reader that also is being actively exploited. Attackers have been observed exploiting these vulnerabilities by sending victims specially crafted PDFs, often attached in a phishing email, that when opened on the victim's machine, the attacker is able to gain arbitrary code execution abilities.

Another zero-day reported by Microsoft, but not actively exploited in the wild, is CVE-2021-31968. Issued a CVSS score of 7.5, this flaw, now patched, could be exploited to trigger a denial-of-service attack.

Microsoft also patched five critical bugs, flaws that can be remotely exploited to seize control over the targeted Windows computer without any help from users. CVE-2021-31959 affects everything from Windows 7 through Windows 10 and Server versions 2008, 2012, 2016 and 2019.

While these vulnerabilities have already been exploited in the wild as zero-days, it is still vital that organizations apply these patches as soon as possible.

Reference(s)	Krebs on Security, Microsoft, ZDNet, Microsoft, Microsoft, Microsoft, Microsoft, Microsoft

CVE(s)
CVE-2021-33742

CVE-2021-31955

CVE-2021-31956

CVE-2021-33739

CVE-2021-31201

CVE-2021-31199

CVE-2021-31959

CVE-2021-31968

Sources
Krebs on Security: Microsoft Patches Six Zero-Day Security Holes

ZDNet: Microsoft June 2021 Patch Tuesday: 50 Vulnerabilities Patched, Six Zero-Days Exploited in the Wild

Alert ID 2b0d1f5f

View Alert

Tags Microsoft Patch Tuesday, Microsoft

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

For Questions or Comments Please email us at toc@h-isac.org