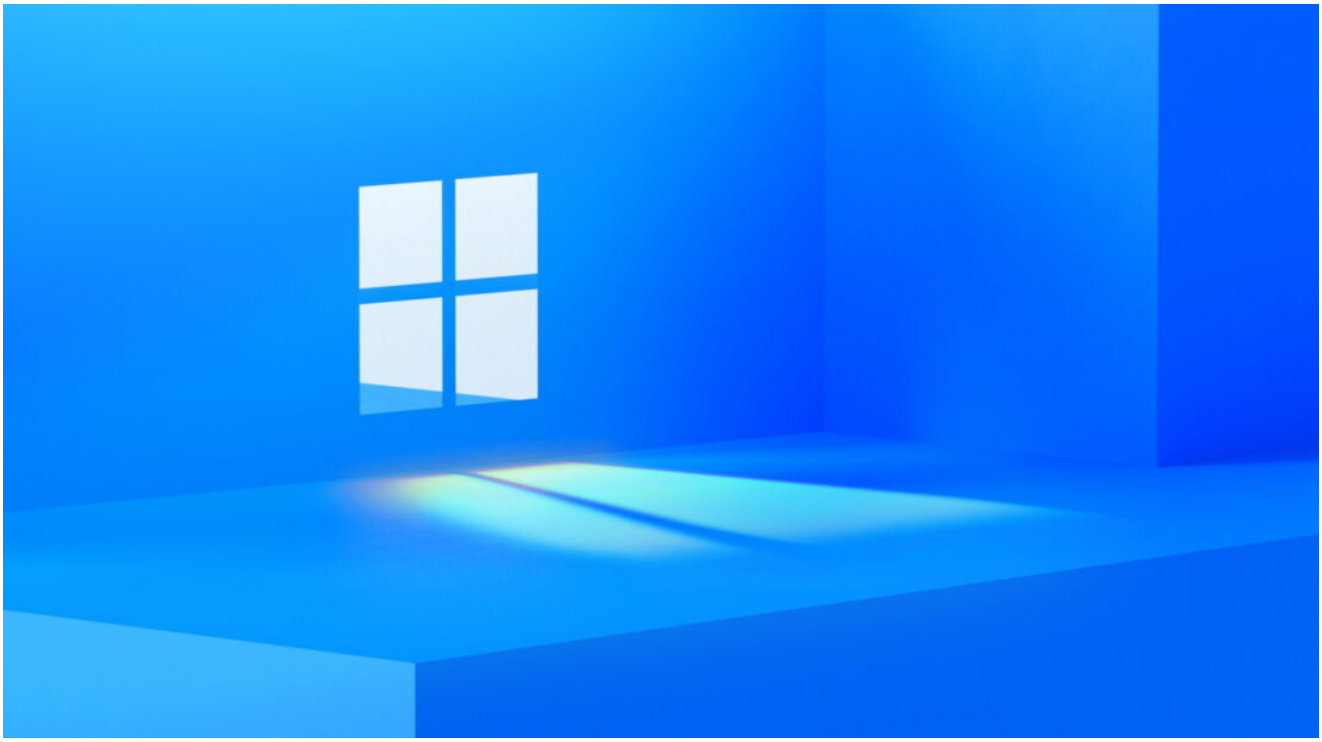
Microsoft patches six Windows zero-days, including a commercial exploit

therecord.media/microsoft-patches-six-windows-zero-days-including-a-commercial-exploit/

June 9, 2021



Microsoft has released today its monthly batch of security updates, known in the industry as Patch Tuesday.

This month's security patches fix 50 vulnerabilities, including six actively exploited Windows zero-days, representing the largest batch of actively exploited zero-days patched in one go in the company's recent history.

- CVE-2021-33742 – Windows MSHTML Platform Remote Code Execution Vulnerability
- CVE-2021-31955 – Windows Kernel Information Disclosure Vulnerability
- CVE-2021-31956 – Windows NTFS Elevation of Privilege Vulnerability
- CVE-2021-31962 – Kerberos AppContainer Security Feature Bypass Vulnerability
- CVE-2021-31199 – Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability
- CVE-2021-31201 – Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability

Details about how the six zero-days have been kept under wraps, as is usually the case with these types of disclosures, primarily to give defenders more time to apply patches before other threat actors can learn how to exploit the bugs.

However, some small details have leaked, from Google and Kaspersky, two of the companies that reported the ongoing attacks to Microsoft in the first place.

CVE-2021-33742: A commercial exploit

The most interesting of the six zero-days is **CVE-2021-33742**, a remote code execution vulnerability in the MSHTML component that is part of the Internet Explorer browser.

In a tweet on Tuesday, Shane Huntley, head of the Google Threat Analysis Group, said his team discovered this vulnerability being abused in the wild and all signs pointed that the exploit appears to have been developed by a professional commercial exploit broker.

While Huntley didn't share technical details about the zero-day, which he promised his team will share in 30 days, the Google TAG head said the exploit appears to have been used by a nation-state for a small number of attacks against targets in Eastern Europe and the Middle East.

> More details will be on CVE-2021-33742 will come from the team, but for context this seem to be a commercial exploit company providing capability for limited nation state Eastern Europe / Middle East targeting.
>
> — Shane Huntley (@ShaneHuntley) June 8, 2021

Two zero-days targeted recent versions of Windows 10

But while Google was able to link the MSHTML zero-day attacks to an exploit broker and a nation-state entity, Kaspersky is still looking for details about two zero-days its researchers caught last month.

Tracked as CVE-2021-31955 and CVE-2021-31956, the Russian security firm said the two Windows bugs were part of a complex exploit chain that also involved a web delivery via the Chrome browser.

"While we were not able to retrieve the exploit used for remote code execution (RCE) in the Chrome web browser, we were able to find and analyze an elevation of privilege (EoP) exploit that was used to escape the sandbox and obtain system privileges," researchers said in a report published today shortly after Microsoft released its Patch Tuesday updates.

Both Windows zero-days, which exploited two distinct vulnerabilities in the Microsoft Windows OS kernel, were particularly interesting because they were fine-tuned to work against the latest and most prominent builds of Windows 10 (17763 – RS5, 18362 – 19H1, 18363 – 19H2, 19041 – 20H1, 19042 – 20H2), suggesting that the threat actor was interested in targeting modern and up-to-date devices.

Two 0-days linked to last month's Adobe Reader zero-day

Additionally, Microsoft also patched two zero-days in CVE-2021-31199 and CVE-2021-31201 that were related to an Adobe Reader zero-day (CVE-2021-28550) that Adobe patched last month in May.

Both zero-days impact one of Microsoft's cryptographic libraries and even impact old versions of Windows, such as 7 and Server 2012.

Unfortunately, neither the Adobe nor the Microsoft patch notes reveal any information about the attacks.

Tags

- Adobe Reader
- APT
- exploit broker
- Google Chrome
- Microsoft
- Patch Tuesday
- vulnerability
- Windows
- zero-day

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.