Memory Bugs Account for Most of Chrome’s 353 New Security Fixes

The update fixes 353 flaws, including 163 memory corruption and 125 use-after-free vulnerabilities.

The post Memory Bugs Account for Most of Chrome’s 353 New Security Fixes appeared first on SecurityWeek.

https://www.securityweek.com/memory-bugs-account-for-most-of-chromes-353-new-security-fixes/

PHP warns it plans to release 2 emergency patches imminently

Website admins, brace yourselves. Fixes for what are believed to be uncommonly severe vulnerabilities are scheduled to drop in a little more than 12 hours for PHP, a programming language that powers websites and Web applications everywhere.

PHP maintainers said Monday that they planned to release patches for two vulnerabilities, both with severity ratings of 9.2 out of a possible 10.

Waiting for PHP2Shell

“All PHP users are encouraged to prepare now so they can

upgrade as soon as the release is available," the advisory stated. "We reserve the right to release earlier should details of either vulnerability become public, or should evidence of active exploitation appear in the wild."

Read full article

Comments

https://arstechnica.com/security/2026/10/php-maintainers-tell-web-devs-to-prepare-themselves-for-critical-security-patches/

Chinese APT Exploited BeyondTrust Vulnerability as Zero-Day

Armory Castle exploited CVE-2026-102764 for initial access, deployed custom tools, and deleted logs and artifacts.

The post Chinese APT Exploited BeyondTrust Vulnerability as Zero-Day appeared first on SecurityWeek.

https://www.securityweek.com/chinese-apt-exploited-beyondtrust-vulnerability-as-zero-day/

F5, Juniper Networks Patch

Critical Vulnerabilities

Successful exploitation of some of these issues could lead to remote code execution and full device takeover.

The post F5, Juniper Networks Patch Critical Vulnerabilities appeared first on SecurityWeek.

https://www.securityweek.com/f5-juniper-networks-patch-critical-vulnerabilities/

Microsoft Patches Two Dozen RCE Flaws in Office

In addition to RCE flaws, Microsoft fixed multiple information disclosure bugs and a security bypass issue in Office.

The post Microsoft Patches Two Dozen RCE Flaws in Office appeared first on SecurityWeek.

https://www.securityweek.com/microsoft-patches-two-dozen-rce-flaws-in-office/

Palo Alto Networks Patches PAN-OS Zero-Day Exploited for

Remote Code Execution

The company says it’s aware of limited exploitation against customers’ firewalls, and it has made IoCs available.

The post Palo Alto Networks Patches PAN-OS Zero-Day Exploited for Remote Code Execution appeared first on SecurityWeek.

https://www.securityweek.com/palo-alto-networks-patches-pan-os-zero-day-exploited-for-remote-code-execution/

Cisco Warns of Exploited Secure Email Gateway Vulnerability

Unauthenticated, remote attackers could write arbitrary files to the operating system and execute commands with root privileges.

The post Cisco Warns of Exploited Secure Email Gateway Vulnerability appeared first on SecurityWeek.

https://www.securityweek.com/cisco-warns-of-exploited-secure-email-gateway-vulnerability/

Chrome, Firefox Updates Patch 114 Flaws as Mozilla Unveils Firefox Enterprise

Mozilla has introduced Firefox Enterprise for organizations with strict compliance, governance, and security requirements.

The post Chrome, Firefox Updates Patch 114 Flaws as Mozilla Unveils Firefox Enterprise appeared first on SecurityWeek.

https://www.securityweek.com/chrome-firefox-updates-patch-114-flaws-as-mozilla-unveils-firefox-enterprise/

Citrix, Fortinet, Ivanti Patch 29 Vulnerabilities Across Their Products

Critical-severity flaws could lead to authentication bypass, code execution, and sensitive authentication information leaks.

The post Citrix, Fortinet, Ivanti Patch 29 Vulnerabilities Across Their Products appeared first on SecurityWeek.

https://www.securityweek.com/citrix-fortinet-ivanti-patch-29-vulnerabilities-across-their-products/

Microsoft Patches Record 1,413 Vulnerabilities, Including Exploited Windows Zero-Day

The most important is CVE-2026-96951, a security feature bypass flaw in Windows that has been exploited in the wild.

The post Microsoft Patches Record 1,413 Vulnerabilities, Including Exploited Windows Zero-Day appeared first on SecurityWeek.

https://www.securityweek.com/microsoft-patches-record-1413-vulnerabilities-including-exploited-windows-zero-day/