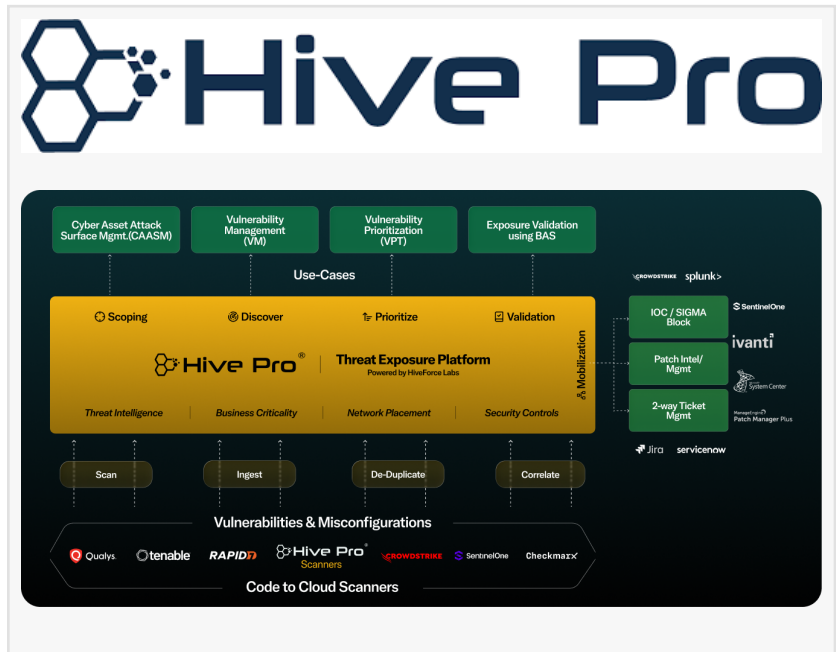


Hive Pro Discovers Four Windows CVEs in October 2026 Patch Tuesday

HiveForce Labs contributes in Microsoft's largest security release ever. Safe attack simulations for Patch Tuesday CVEs are live on the Hive Pro platform.

HERNDON, VA, UNITED STATES, October 20, 2026 /EINPresswire.com/ -- Hive Pro, the Continuous Threat Exposure Management (CTEM) company, today announced that HiveForce Labs, its threat and vulnerability research unit, discovered four Windows vulnerabilities fixed in Microsoft's October 2026 Patch Tuesday. Read the [detailed blog](#).



That release, published October 13, fixed 1,413 Microsoft CVEs. It is the first Patch Tuesday to cross 1,000 and beat September's record of 974 by roughly 45 percent. Windows alone accounted for 1,102 fixes, and one Windows Shell zero-day, CVE-2026-96951, was already exploited in the wild.

Four flaws in tools every Windows machine ships with

Microsoft's Security Update Guide credits the discoveries to Owais Lone, Senior Threat Researcher at HiveForce Labs. Three affect Microsoft OpenSSH for Windows (ssh, scp and sftp). The fourth affects the Windows build of libarchive behind the built-in tar.exe.

- CVE-2026-83923: OpenSSH for Windows path traversal, remote code execution (CVSS 8.8)
- CVE-2026-88157: OpenSSH for Windows heap overflow, remote code execution (CVSS 8.8)
- CVE-2026-83754: OpenSSH for Windows heap overflow, remote code execution (CVSS 7.5)
- CVE-2026-69968: Windows libarchive (tar.exe) path traversal, tampering (CVSS 6.5)

"The people who live in ssh, scp and tar are developers, admins and build systems, and their machines hold source code, credentials and signing keys," said Owais Lone. "I went where the crowd is not: Microsoft's OpenSSH porting layer, which upstream never reviews, and an inbox tar.exe missing a fix already sitting in libarchive's master branch."

AI is accelerating discovery, for both sides. The record volume is no accident. Monthly CVE disclosures grew about 145 percent between June 2024 and June 2026, and Microsoft has credited large language models for much of this year's discovery volume. Microsoft has now passed 4,000 CVEs in 2026 with two months to go.

"AI has collapsed the time between a bug existing and someone finding it, and attackers have the same agents we do," said Sarfaraz Kazi, Co-Founder and CTO of Hive Pro. "When one month brings more than 1,400 CVEs, a severity score cannot tell you what to fix first. Exposure validation can. Prove what an attacker can actually do in your environment with evidence, then fix that."

The only vulnerability attackers were exploiting in the wild this month, CVE-2026-96951, was rated Important, not Critical, with a CVSS score of 8.8. Meanwhile, 78 other flaws in the same release earned a Critical rating with no known exploitation. A team patching by severity score would have queued the one vulnerability under active attack behind 78 others. CVSS measures theoretical damage, not what an attacker can do in your environment. The four HiveForce Labs CVEs carry the same Important rating, leaving code execution on developer laptops and build servers waiting in line while attackers read the same release notes.

Hive Pro recommends a Mitigate First, Patch Faster approach to a patch load no team can clear in a single cycle. Confirm where you are exposed, cut the risk immediately, then patch as fast as your change process allows.

For these four CVEs, interim mitigations include avoiding recursive scp and sftp downloads from untrusted servers, extracting outside archives as a standard user in an empty folder, removing the symbolic-link privilege from accounts that unpack third-party archives, and keeping Windows' built-in terminal support switched on.

Hive Pro customers can act today:

- Discover: Predicted CVEs show whether the four vulnerabilities are present, with no scan required.
- Validate: Safe Breach and Attack Simulation (BAS) exploits for all four CVEs are live in the Hive Pro platform, so teams can test whether their controls stop them.
- Prioritize the zero-day: a BAS simulation for CVE-2026-96951, the Windows Shell Mark of the Web bypass on CISA's Known Exploited Vulnerabilities list, is also available.

"Most enterprises cannot patch 1,400 CVEs in a month, and they should not try to in severity order," said Kazi. "Our customers could test their defenses against these four CVEs from the day Microsoft disclosed them. That is the gap between knowing about a vulnerability and knowing whether it can hurt you."

Research that feeds the platform.

HiveForce Labs is Hive Pro's threat and vulnerability research unit. Its researchers track active threats, hunt for new vulnerabilities in widely deployed software, and turn findings into safe, testable attack simulations. The October CVEs join a growing BAS library of zero-days, N-days,

CVE exploits and advanced attack chains that customers can run against their

Marketing

Hive Pro

marketing@hivepro.com

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/950694047>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.