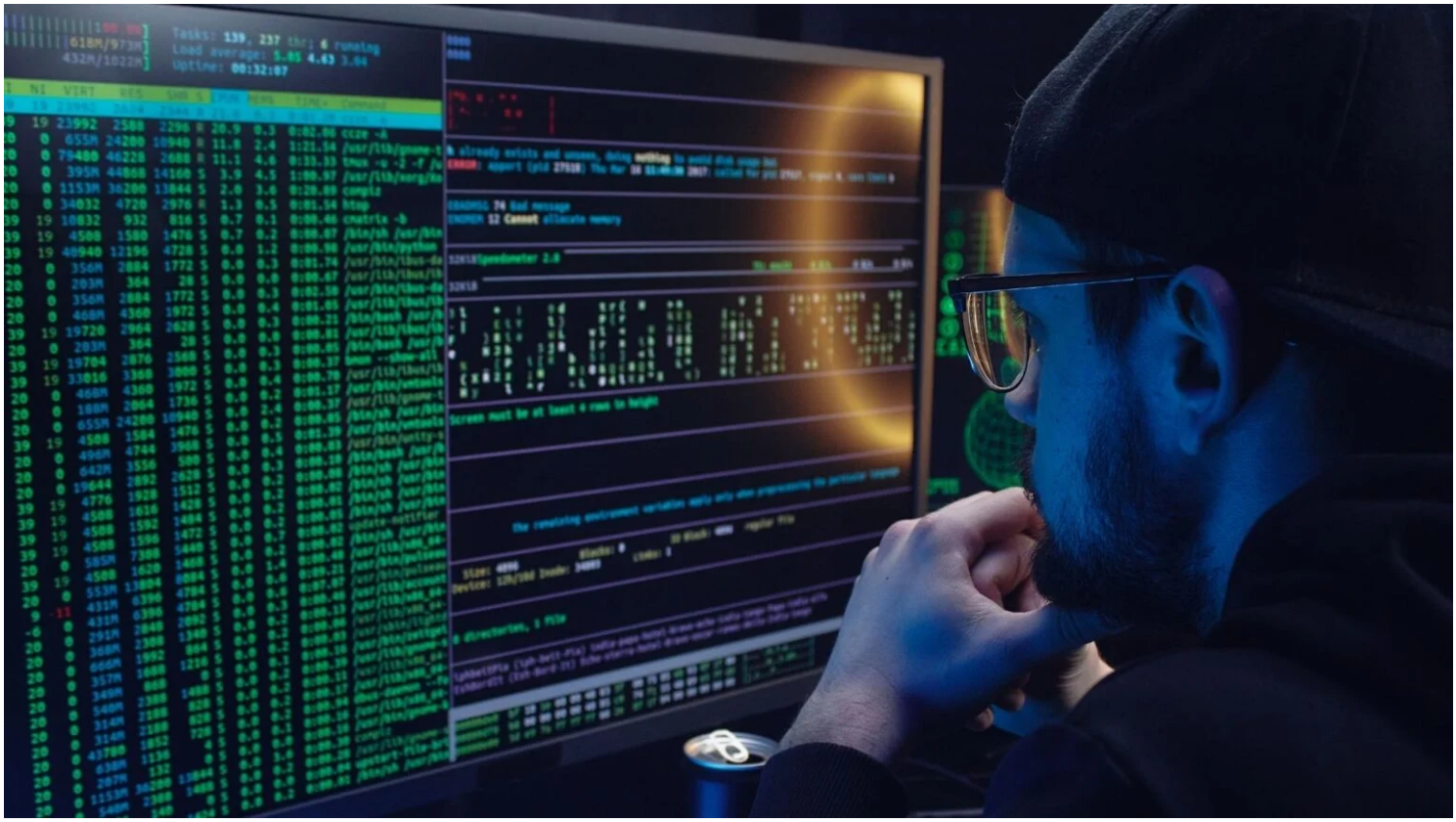

Warning: A new vulnerability (CVE-2022-47966) can allow attackers to gain high, system-level access without authentication.

CVE-2022-47966 represents a significant enterprise threat by impacting products like ServiceDesk Plus, Active Directory 360, and more. The vulnerability is now publicly available and allows attackers to access a system via remote code execution and gain control without the need for authentication.

Experts report that the vulnerability is alarmingly simple for attackers to exploit, especially for use in “spray and pay” assaults. It is suspected that the vulnerability stems from susceptible, third-party dependencies and breaches are being detected for those who haven’t patched affected products. By gaining full control of a system, attackers can threaten all credentials stored in an application or dump them by utilizing Local Security Authority Server Service (LSSASS)

(https://en.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Service#:~:te
Additionally, the vulnerability allows attackers easy access to customer environments.

Fortunately, Covestic has a solution to help organizations better protect themselves from vulnerability threats. With ActivateVR, customers can successfully prioritize and remediate critical vulnerabilities quickly and effectively. Contact us (https://www.covestic.com/contact/) today to learn more about how ActivateVR can be a vital asset in protecting your operations.
Categories: Cybersecurity (https://www.covestic.com/blog/category/cybersecurity/), ServiceNow Security Operations (https://www.covestic.com/blog/category/servicenow-security-operations/)

PREVIOUS POST (HTTPS://WWW.COVESTIC.COM/BLOG/TOKYO-RELEASE-HI
BACK TO BLOG
(HTTPS://WWW.COVESTIC.COM/BLOG/)
JR-SERVICENOW-ADVISORY-SERVICES-DIGITAL-TRANSFORMATION-ROADMAP/)

Contact us for a free consultation.