CYBER ADVISORY

Friday, December 12, 2025 **CAL-CSIC-202512-A-006**

IceWarp Vulnerability enables RCE bypassing authentication

Multiple Sectors impacted	IceWarp14.x	Remote Code Execution	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical Remote Code Execution (RCE) vulnerability in affected installations of IceWarp server 14.x. CVE-2025-14500 carries a CVSS 3.1 score of 9.8. Successful exploitation of CVE-2025-14500 allows remote attackers to execute arbitrary code, and authentication is not required to exploit this vulnerability.

This flaw occurs from improper sanitization of user-supplied input within the application's X-File-Operation request handling logic; enabling an attacker to craft malicious requests that inject arbitrary code, which can result in remote code execution (RCE) in the context of SYSTEM. Exploitation of this vulnerability can lead to direct access to email, file storage, conferencing systems and user authentication data enabling further lateral movement within the victim's infrastructure. Researchers at Zero Day Initiative have publicly released a Proof-of-Concept (PoC)[1]. There is a patch provided by the vendor.[2]

Affected Products	Vulnerable Versions	Safe/Patched Version (Minimum Required)	Recommended Action
IceWarp Epos Update 2 (Latest Generation)	All versions before 14.2.0.9	14.2.0.9 or newer	Urgent Upgrade
IceWarp Epos Update 1	All versions before 14.1.0.19	14.1.0.19 or newer	Urgent Upgrade
IceWarp Epos (1st Gen)	All versions before 14.0.0.18	14.0.0.18 or newer	Urgent Upgrade
Deep Castle (Older Major Version)	All versions before 13.0.3.13	13.0.3.13 or newer	Urgent Upgrade

The Cal-CSIC recommends immediately deploying the latest security update to affected IceWarp servers.

For further information on applying the vendor's security patch please use this link: **IceWarp Security Update**

References

[1] Zero Day Initiative; IceWarp14 X-File-Operation Command Injection Remote Code Execution Vulnerability; https://www.zerodayinitiative.com/advisories/ZDI-25-1072/; accessed 12 December 2025
[2] IceWarp; IceWarp Security Update; https://support.icewarp.com/hc/en-us/articles/39702252317713-IceWarp-Security-Update; accessed 12 December 2025