Advisory on Savannah lwIP SMTP Client Vulnerability



A critical vulnerability in the Savannah lwIP SMTP client could lead to remote code execution due to a buffer overflow. Institutions using affected versions should take immediate action to mitigate risks.

- Affected version: Savannah lwIP SMTP client 2.2.1.
- Vulnerability allows for potential remote code execution.
- Critical impact on sectors such as Energy and Water.
- Mitigation patch is available for the vulnerability.
- Immediate action is recommended for affected institutions.

Overview

The Savannah lwIP SMTP client has been identified with a critical vulnerability that could allow for remote code execution through a buffer overflow. This issue affects version 2.2.1 and poses significant risks to critical infrastructure sectors, including energy and water systems.

Vulnerability Details

The vulnerability arises from the lwIP SMTP client not adequately checking the size of inputs, leading to a buffer overflow condition. This could potentially crash the device being accessed, making it imperative for organizations to assess their systems for this vulnerability.

Recommended Actions

Organizations utilizing the affected version of the Savannah lwIP SMTP client should take the following actions to mitigate risks:

- Update to the latest version of the Savannah lwIP SMTP client as soon as possible.
- Apply the available patch (patch_125_smtp_txbuf.diff) to address the vulnerability.
- Conduct a thorough review of systems to identify any instances of the affected client.
- Implement monitoring to detect any unusual activity that may indicate exploitation attempts.
- Ensure that all relevant personnel are informed about the vulnerability and the steps taken to mitigate it.

What to do now

1. Update to the latest version of the Savannah lwIP SMTP client.
2. Apply the patch provided to fix the vulnerability.
3. Review systems for instances of the affected client.
4. Implement monitoring for unusual activity.
5. Inform relevant personnel about the vulnerability.