مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

# Critical Vulnerability in F5 Platforms

Tracking #:432317810

Date:14-10-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed F5 has disclosed a critical vulnerability (CVE-2023-28863) impacting systems utilizing AMI MegaRAC SPx12 and SPx13 firmware for Intelligent Platform Management Interface (IPMI).

## TECHNICAL DETAILS:

F5 has disclosed a critical vulnerability (CVE-2023-28863) impacting systems utilizing AMI MegaRAC SPx12 and SPx13 firmware for Intelligent Platform Management Interface (IPMI). The flaw stems from insufficient verification of data authenticity, allowing a remote attacker with network access to bypass integrity and confidentiality protections negotiated in IPMI v2.0 sessions. This could enable unauthorized access to the Always-On Management (AOM) subsystem and compromise platform-level security controls on affected devices.

**Vulnerability Details:**

- **CVE ID:** CVE-2023-28863
- **Severity-**9.1 Critical
- **Vulnerability Type:** Insufficient Verification of Data Authenticity
- **Component:** Intelligent Platform Management Interface (IPMI) – AMI MegaRAC SPx
- **Impact:**
  Attackers with network access could bypass IPMI session security parameters (integrity and confidentiality), potentially allowing:
- Unauthorized access to the management interface
- System manipulation or firmware-level compromise
- Exposure of management credentials or sensitive operational data
- **Affected Platforms:**
  - i2000 (C117)
  - i4000 (C115)
  - i5000 (C119)
  - i7000 (C118)
  - i10000 (C116)
  - i11000 (C123)
  - i15000 (D116)

## RECOMMENDATIONS:

Organizations using affected F5 devices should immediately assess exposure, disable unnecessary IPMI services, and isolate management interfaces while awaiting permanent fixes.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:


- https://my.f5.com/manage/s/article/K000156992?utm_source=f5support&utm_medium=RSS