مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in Siemens InterMesh Subscriber Devices

Tracking #:432316467

Date:05-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple severe vulnerabilities have been discovered in Siemens InterMesh Subscriber Devices, potentially allowing unauthenticated remote attackers to execute arbitrary code with root privileges.

TECHNICAL DETAILS:

InterMesh Subscriber devices are currently affected by multiple vulnerabilities including a critical vulnerability that enable unauthenticated remote attackers to execute arbitrary code with root privileges. The highest risk is associated with specific versions of the InterMesh 7177 Hybrid and 7707 Fire Subscriber products.

Key Vulnerabilities:

- CVE-2024-47901 (CVSS v3.1: 10.0): Allows remote code execution through unsanitized input.
- CVE-2024-47902 (CVSS v3.1: 7.2): Enables unauthenticated execution of system commands.
- CVE-2024-47903 (CVSS v3.1: 5.8): Permits arbitrary file writes to the web server's directory.
- CVE-2024-47904 (CVSS v3.1: 7.8): Facilitates local privilege escalation to root.

Affected Product	Versions	Remediation
InterMesh 7177 Hybrid	All versions < V8.2.12	Update to V8.2.12 or later
InterMesh 7707 Fire Subscriber	All versions < V7.2.12 (IP interface enabled)	Update to V7.2.12 or later and disable IP interface

RECOMMENDATIONS:

- Immediate Update: All users of affected InterMesh devices should update to the latest versions as soon as possible.
- Access Restrictions: Implement access control measures to restrict network access to trusted systems and users only.
- Disable Unused Interfaces: For devices where the IP interface is not needed, it should be disabled to reduce exposure.

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://cert-portal.siemens.com/productcert/html/ssa-333468.html