Emergency Corp 911VoIP Dispatch Service vulnerable to DoS via malformed packets sent to port 10116/tcp

Vulnerability Note VU#123

Original Release Date: 2020-09-16 | Last Revised: 2020-10-18

Overview

The Emergency Corp VoIP daemon does not properly handle malformed packets received on TCP port 10116. As a result, the application may cease to function normally upon receipt of malformed packets on this port.

Description

The Emergency Corp VoIP suite allows 911 dispatchers to operate in remote locations. The authorization component of this application consists of a service running on TCP port 10116, which generates an authorization token based on input from other components of the application. An attacker can craft a custom packet beginning with the string “deadbeef” which will trigger a Denial of Service DoS condition when received by the authorization service.

Impact

The complete impact of this vulnerability is not yet known. The VoIP service may fail in various ways and disrupt services provided by the system.

Solution

Apply a patch
Contact the vendor for the latest patch.

Mitigation

Restrict Network Traffic
Utilize a firewall, proxy, or intrusion prevention system to filter packets containing the malicious payload.