# LAVELLE NETWORKS

Security-Vulnerability Policy

Purpose

This policy was created to guide and inform Lavelle Networks customers in the event of a reported vulnerability in a Lavelle Networks product or cloud-hosted service. It ensures that Lavelle Networks customers understand how Lavelle Networks responds to events of this nature by Lavelle Networks Security Incident Response Team (LN-SIRT)

Lavelle Networks' Response Process
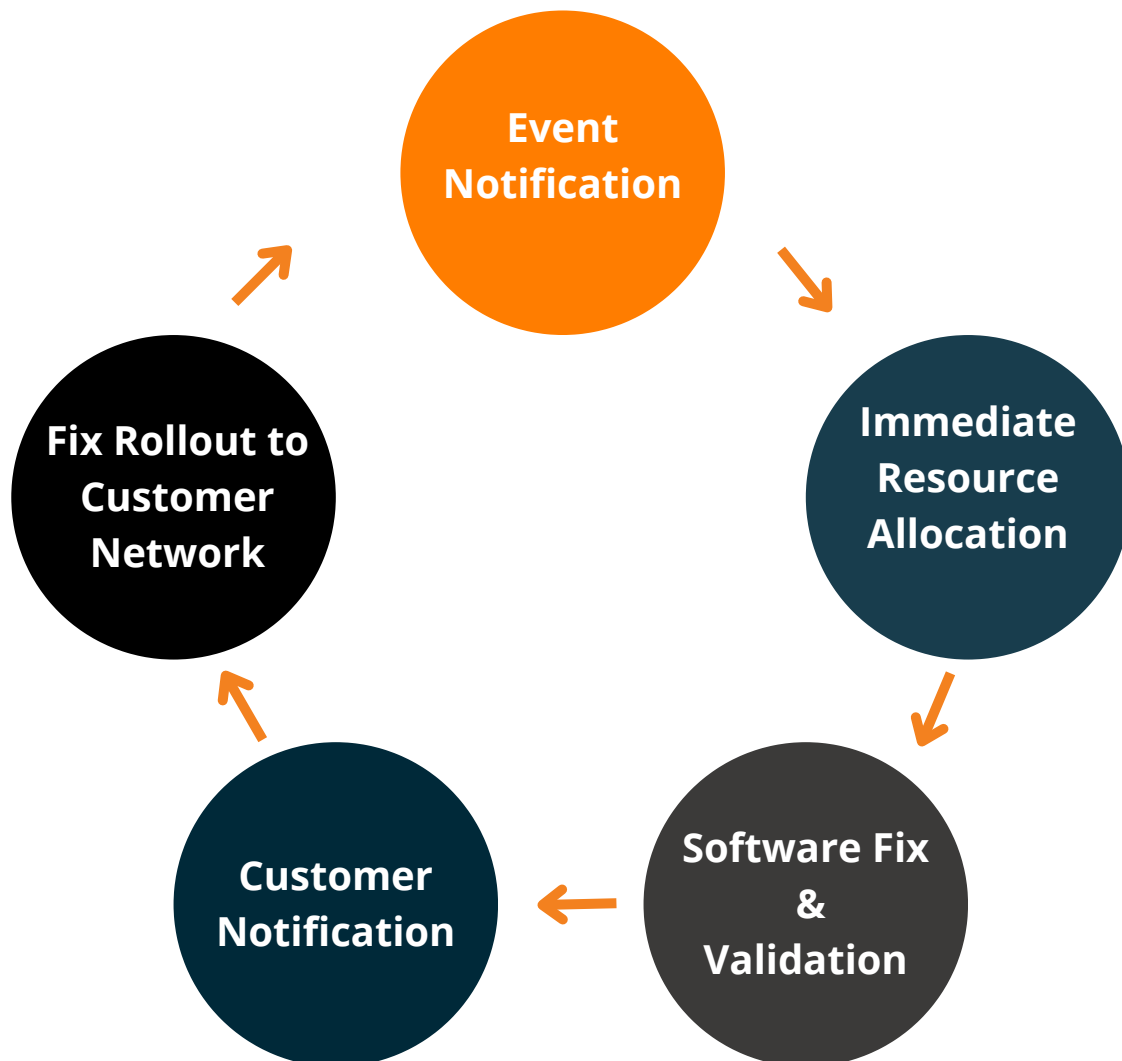
**The steps in the process illustrated are as follows:**

- **Event Notification:** LN-SIRT receives notification of a security incident.

- **Immediate Resource Allocation:** LN-SIRT prioritizes and identifies resources.

- **Software Fix & Validation:** LN-SIRT coordinates the development and internal lab validation of the fix.

- **Customer Notification:** LN-SIRT notifies all affected customers simultaneously.

- **Fix /Rollout to Patch Network**

The LN-SIRT investigates all reports regardless of the software code version or product life cycle status until the product reaches the End-of-Support (EoST). Issues will be prioritized based on the potential severity of the vulnerability. Ultimately, the resolution of a reported incident may require upgrades to products and cloud-hosted services that are under active support.

LN-SIRT Team Composition

During any investigation, Lavelle Networks manages all sensitive information on a highly confidential basis. Internal distribution or communication is limited to those individuals who are authorized and approved to work on an issue.

Engineering

Customer ← LN-SIRT → Product

Support
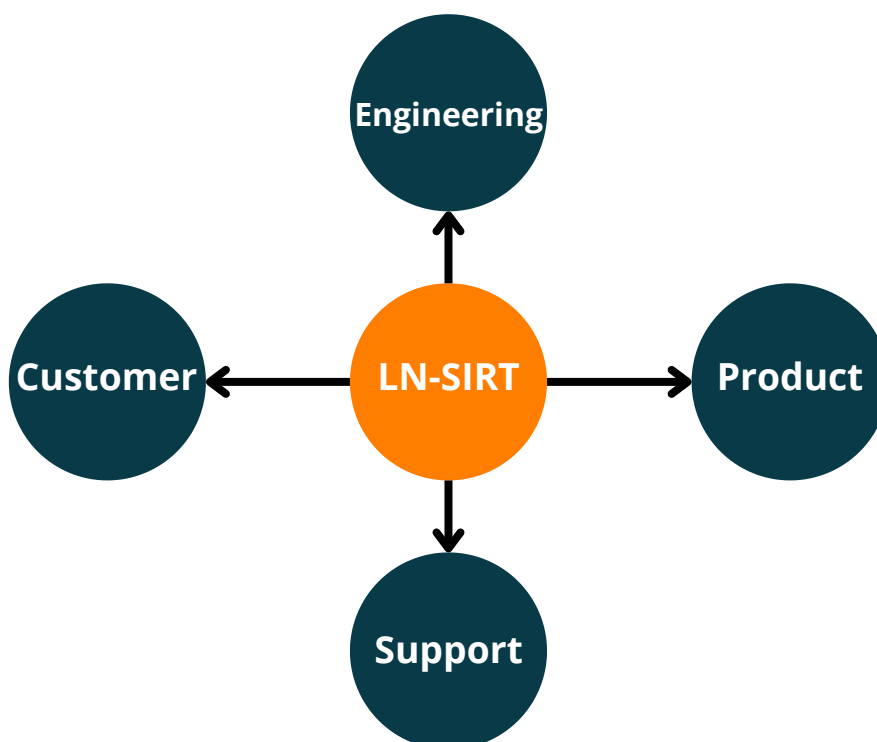
To ensure this process, LN-SIRT is comprised of two groups: Incident Response Managers (IRMs) and Security Incident Response Engineers (SIRE).

Incident Response Managers (IRMs)

- The goal of IRM is to handle any Security Incident from its report/identification time till resolution, working with SIRE, Sales, Customer and Any external incident reporter.

- The IRM role is also to share the findings post resolution and be the custodian of the database of Vulnerabilities.

Security Incident Response Engineers (SIRE)

- Role of SIRE is to immediately work in a lab environment, replicating whenever possible all discovered security vulnerabilities.

- SIRE also performs additional testing to confirm that the fixes do indeed repair the affected product.

- They also create a knowledge base, share observations to Product and Engineering teams to keep them updated.

Fixing Vulnerabilities

While Lavelle Networks strives to fix all security vulnerabilities as quickly as possible, we use CVSS (Common Vulnerability Scoring System) scoring to prioritize the security vulnerabilities to be resolved and merge the resulting fixes into the mainline. The fixes could be a patch / OS / software upgrade depending on the root cause of the issues.

Table 1: CVSS Score Determines Scope and Priority of Security Bug Fixes

CVSS Score	Qualitative Rating	1st Response TAT (max duration)	TAT for Workaround (as applicable)	TAT for Closure (max duration)
< 3.9	Low	72 Hours	96 Hours	90 Days
4.0 to 6.9	Medium	48 Hours	72 Hours	60 Days
7.0 to 8.9	High	12 Hours	48 Hours	15 Days
9.0	Critical	2 Hours	24 Hours	5 Days

To report any incident please mail to LN-SIRT@LAVELLENETWORKS.COM

LAVELLE NETWORKS

Accelerate Networks for the Digital Economy

Top Global enterprise brands are using
Lavelle Networks SD-WAN platform for upgrading their
infrastructure to next generation WAN and hybrid WAN
Solutions.
We have crossed 20,000+ SDWAN deployments in India.

WWW. LAVELLENETWORKS.COM

Speak to our experts

Web: www.lavellenetworks.com/contact/
Email: sales@lavellenetworks.com

ATM Networks of top Banks	Top Public Sector Mutual Fund Brands	Premier Co-operative Banks
Largest NBFCs	Top Insurance Companies	Largest e-commerce Networks

ScaleAOn® - Networks at Scale, Always ON

We deliver the best enterprise network experience