Prior to contacting Avaya regarding a security issue, check actions below based on type of Security request.

**Contact Customer Support using the contact information at** https://support.avaya.com/contact/ or create a Service Request (SR) at https://support.avaya.com/service-requests/

**Security request type**

- **Active Attack**
  - Disconnect the equipment from the network, but do not shut it off. Contact law enforcement.

- **Toll Fraud**
  - Experiencing active Toll Fraud on Avaya system.

- **Request for Security Services**
  - Request security services (server hardening, compliance work, scans, firewalls, etc.)

- **Operational Security Questions**
  - General questions about Avaya’s internal security policies

- **Vulnerability Concerns about an Avaya Product**
  - Review vulnerability data

**Avaya does not provide forensic services, however will participate as appropriate in investigations.**

**Avaya Professional Services (APS)**

- Request security services through sales channels:
  - New install – security acceptance
  - Existing deployment – security assessment
  - Existing deployment – hardening request

- APS reviews security service request and provides quote for service.

- If contract with Avaya for security services, security service is provided.

**VULNERABILITY CONCERN (NOT AN ATTACK)**

- Review vulnerability data
- Search support.avaya.com using a keyword for the vulnerability, e.g. RHSA-2015-0674, CVE-2014-8159, kernel, MS15-061, etc.

- Refer to PCN and/or PSN for mitigation of the security issue. If only an ASA exists, refer to the product actions for details of the mitigation plan.

- Does an ASA, PCN or PSN document exist?
  - Yes
    - Refer to PCN and/or PSN for mitigation of the security issue.
  - No
    - Vulnerability details a scan report?
      - Yes
        - Avaya Support Team member will be in contact.
      - No
        - Create a Service Request (SR). Provide detailed information about the product, product version, vulnerability and any other important information necessary for proper security escalation handling.

- Standard maintenance does not include interpretation of raw vulnerability scan reports. Contract with an outside company or engage Avaya Professional Services (APS).

- Reference policy on support.avaya.com.

- Information about Avaya’s security mitigation and classification refer to:
  - Avaya’s Product Security Vulnerability Response Policy and Avaya’s Security Vulnerability Classification