Ecessa Security Vulnerability Policy

April 2016

Ecessa solutions are in integral part of your network and must meet or exceed all aspects of your corporate security requirements, policy, and reputation. This security vulnerability policy was created to explain how we are making sure that your solutions are secure and meet new and increasingly stringent testing standards. We take this responsibility seriously and look forward to your feedback.

AWARENESS

Ecessa's internal team actively monitors the forums that are most relevant to our solutions. Every Ecessa product is an x86 based industrial computer running Gentoo Linux. We monitor the Gentoo Security Database (https://security.gentoo.org/) and the NIST National Vulnerability Database (https://nvd.nist.gov/home.cfm) on a monthly basis to determine what new threats are reported.

Our team also monitors relevant social media forums like Twitter, LinkedIn, Facebook, and Google+ daily for mention of any new threats or trends in our industry. New alerts are captured as a new task in Jira, our internal development environment, for our teams to review, assign, and escalate.

ASSESSMENT

Ecessa has an internal, automated testing platform designed to determine if and how each security vulnerability impacts our software code base. First we port the latest security vulnerability code from the Gentoo Linux community, then we load this into our Jenkins automated test platform and execute all tests. The results from this screening output a threat report that indicates if any items affect our software, which ones, and in what way. This report is then reviewed by the development team and any relevant issues are then capture in Jira and assign for a comprehensive team review.

MITIGATION

After the reviews are complete and the threat is verified to impact the Ecessa software code base, our team investigates a solution; this includes understanding the specifics of the threat, the impact on our features, how broadly it impacts our code and kernel, and the best way to mitigate it. Depending on the severity, impact, complexity, and risk the team will generate short and long term options for customers. These options may be limited to communications, indicating a low risk or impact, or be immediate software code updates and release to resolve critical or high risk issues. All software design information associated with the vulnerability and how to mitigate it are updated in the Jira tool.

COMMUNICATIONS

Ecessa has several ways to communicate with our install base customers, new clients, and partner groups. Each communication path is provided to accommodate different communication needs, styles, details, and frequency. Below are the three levels of communications

- **Public**
  One-time notices are published to the following medium at time of mitigation completion; general public can also see additional content listed below:
  - Ecessa main website (www.ecessa.com)
    - Security
      - Policy
      - Latest threats
      - Alerts and recommendations
  - Ecessa Support website (support.ecessa.com)
    - Announcements
      - Articles on specific CVE threats
      - Links to FAQs
      - Links to mitigation steps
- **Install Base**
  - Device Graphic User Interface (GUI) notifications
    - Alerts for users when new versions of software are available for upgrade
      - Each software revision has release notes that indicate which CVE is addressed and how it corrects the issue.
  - Cloud View Alerts (Available in Q4 2016)
    - Alerts can be configured through the Ecessa Cloud View web application
      - Each CVE that potentially impacts Ecessa products, features, or functions will have a message that details impact, mitigation, and next steps for customers.
- **Partners**
  - Public Alerts (detailed above)
  - Install Base Alerts (if applicable)
  - E-mail Alerts
    - Partners can opt-in to an e-mail alert program with Ecessa. We will send the same information provided in other locations within a single, direct e-mail.
      - E-mails are sent at the same time public alert information is released.
      - E-mail addresses are maintained within our Customer Relations Management (CRM) tool.
      - Partners can request inclusion to this list by sending an e-mail to any of the following:
        - voc@ecessa.com
        - tplant@ecessa.com
        - msiegler@ecessa.com

FEEDBACK

Ecessa has a philosophy of continuous improvements; we are looking to make our products, processes, and experience better each day. To accomplish this, we have a formal Voice of Customer (VoC) process that is open to all customers and partners (voc@ecessa.com). This is also used for us to improve our security vulnerability process and fine tune it for our customers' ever changing needs. Please provide feedback at that e-mail for specifics on this policy or other Ecessa features and products – thank you.