- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Email Security

Malicious Emails Can Crash Cisco Email Security Appliances

By Eduard Kovacs on February 17, 2022

Cisco this week informed customers that its Email Security Appliance (ESA) product is affected by a high-severity denial of service (DoS) vulnerability that can be exploited using specially crafted emails.

The flaw, tracked as CVE-2022-20653, affects the DNS-based Authentication of Named Entities (DANE) email verification component of Cisco AsyncOS Software for ESA. It can be exploited remotely without authentication.

The vulnerability is caused by insufficient error handling in DNS name resolution, Cisco said in its advisory.

“An attacker could exploit this vulnerability by sending specially formatted email messages that are processed by an affected device,” the company explained. “A successful exploit could allow the attacker to cause the device to become unreachable from management interfaces or to process additional email messages for a period of time until the device recovers, resulting in a DoS condition. Continued attacks could cause the device to become completely unavailable, resulting in a persistent DoS condition.”

While the vulnerability sounds serious, it’s worth noting that it only impacts devices that have the DANE feature enabled and downstream mail servers configured to send bounce messages. Cisco noted that the DANE feature is not enabled by default.

Patches and workarounds have been made available, and Cisco has advised customers to deploy them in order to prevent potential exploitation.

Cisco has credited several people working with Dutch government ICT services provider DICTU for reporting the security hole.

The networking giant says there is no evidence of malicious exploitation.

Cisco this week also released two advisories that inform customers about medium-severity issues affecting Cisco RCM for Cisco StarOS software (DoS vulnerability), and Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (XSS vulnerability).

Related: Cisco Patches Critical Vulnerabilities in Small Business RV Routers

Related: Over 70 Vulnerabilities Will Remain Unpatched in EOL Cisco Routers

Related: Cisco Patches Critical Vulnerability in Contact Center Products

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia’s security news reporter. Eduard holds a bachelor’s degree in industrial informatics and a master’s degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

Intel Software and Firmware Updates Patch 18 High-Severity Vulnerabilities
Malicious Emails Can Crash Cisco Email Security Appliances
Russian Cyberspies Stole U.S. Defense Data in Attacks on Contractors
Cybersecurity M&A Roundup for February 1-15, 2022
Ransomware-Related Data Leaks Nearly Doubled in 2021: Report

Tags:
NEWS & INDUSTRY Email Security Vulnerabilities