IronMail 5.0.1 Vulnerable to SYN Attack (DoS)
(Multiple Flood Connections)
Security Advisory

Date
November 29, 2005 – Research and Testing
Junary 10, 2006 – Update Release

Vulnerability
SYN attack Denial of Service (Flood Connections)

Severity
High

Affect Products
IronMail 5.0.1

Local/ Remote
Remote

Vendor Status
Not response yet

Reference about the product
http://www.ciphertrust.com/products/cclass/

Credit
Alex Hernandez, (Bug Hunter)
Mark Ludwik, (Researcher)

Contact
Mark Ludwick [at] d-fender.com

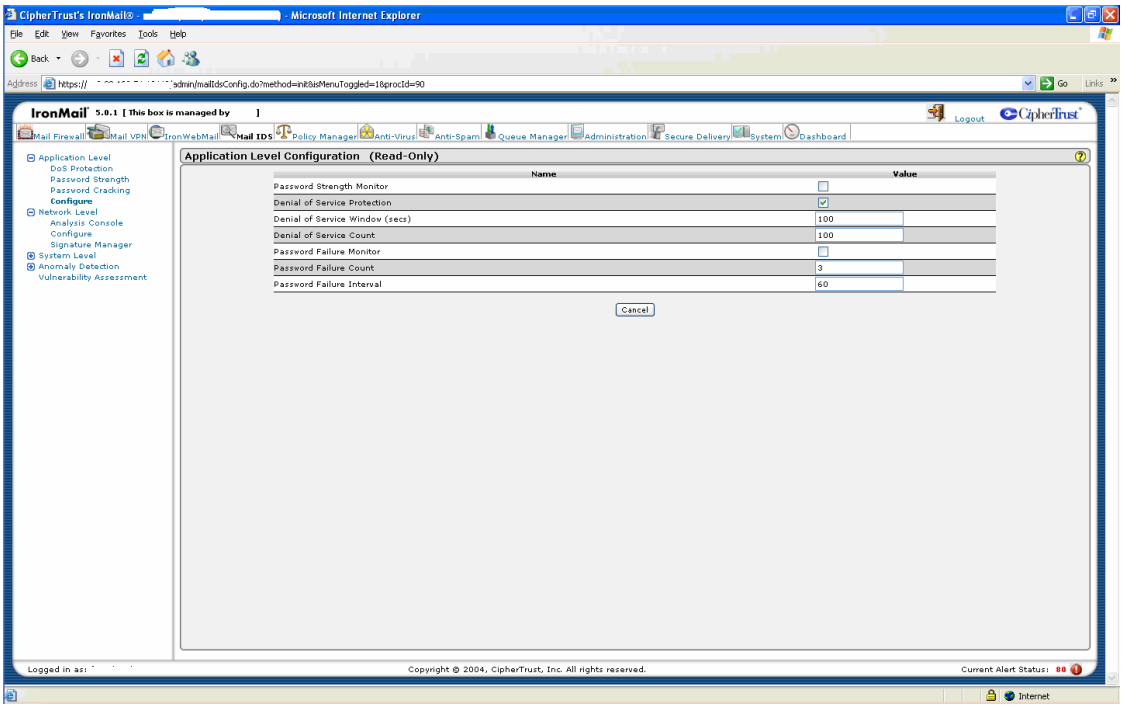
IronMail 5.0.1 Vulnerable to SYN Attack (DoS)
(Multiple Flood Connections)
Security Advisory

Description

The IronMail C-class is designed to handle the email traffic of the most demanding email environments in the world, including ISPs and multinational corporations with several geographically dispersed gateways.

Vulnerability Description

If the IronMail being is configured to reply with a “Denial of Service Window (secs)” field consisting of a string between 100 to N by default and “Denial of Service Count” 100 to N.



Proof of Concept

You can use **hping** or **perl** scripts to created malformed packets and multiple connections. The service remains busy and not blocks the DoS DDoS attacks.