CNS /Update Newsletter Feature

Information Security Incident Tracking Successful

EI&O Document ID: u0505f
Last Updated: 05/01/2005

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
## Table of Contents

Information Security Incident Tracking Successful ..................................................... 3  
For More Information ............................................................................................... 3
Information Security Incident Tracking
Successful

The new information security incident tracking system, implemented in January, is successful at improving incident management and helps to ensure that incidents are resolved in a timely manner.

One goal of the "tickets," which are distributed to network and server managers of compromised hosts, is to provide the security team with a mechanism for accountability. The UF IT Security Team [http://infosec.ufl.edu/] can track which units receive tickets, incident types, and how long it takes them to contain and resolve incidents.

"The ticket tracking system is a uniform and controlled way in which we can assure compromised machines get fixed," said Mark Kovacic, UF Network Security Engineer. "The sooner a ticket is closed, or resolved, the sooner we can be assured that the host is no longer a threat to other resources."

Any network and server managers with tickets older than three days are sent a reminder. The UF IT Security Regulations [http://www.it.ufl.edu/policies/] state that all information security incidents must be contained during the same business day that the notification is received and resolved by Friday of the same week. If an incident is not contained quickly, a filter might be applied to block network access from the host. UF administration will review ticket status reports in order to make more information decisions about the UF IT security program.

The UF IT Security Team would like to thank all network and server managers who have been closing their tickets in a timely manner. Graphs that show unit incident trends are available to authorized network and server managers at https://infosec.ufl.edu/cgi-bin(graphing.

For More Information


Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
Information Security Incident Tracking
Successful

(352) 392.2061
<editor@cns.ufl.edu>