TECHNICAL WHITE PAPER

Oryx Pecos and Unix/Linux Platform Virus Susceptibility

Version: **1.0**

Date: **December 4, 2001**

CID: **90987**

Author: **Rick Robinson**
CES Security Team

Scope of Discussion
With the recent wave of viruses and threats against computers, there is a heightened desire to understand the susceptibilities of DEFINITY® platforms. This document discusses the vulnerabilities of two of those platforms, the Oryx Pecos and Unix/Linux operating systems (OS), against viruses that have recently surfaced.

Discussion
Over the past few months, viruses such as Code Red, Nimda, and BadTrans have made headlines due to the large-scale impact they have had on the business community. Each threat represents a new mechanism to compromise an application or element of the OS. However, each of the viruses attacks only Windows-based platforms. As such, the Oryx-Pecos and Unix/Linux platforms are not susceptible to these viruses.

Windows platforms have historically been the primary target for malicious software. The proliferation of the OS and the availability of tools have provided the means to create malicious applications with relatively little effort.

In addition to the differences in OS, there are characteristics of the DEFINITY/Oryx Pecos platform design that make the system more resilient to attack. They include a lack of co-residency of a web server or email, which greatly reduces the chances of infection. Also, all of the IP interfaces are logically separated from the OS and communicate through a proprietary backplane infrastructure to the OS. This minimizes the opportunity for a line-card infection to even get to the OS. Finally, the only non-administration, non-backplane messaging the OS responds to is a complete code-base rebuild or DEFINITY patches.

Avaya recommends that it's customers pursue good networking practices to isolate host systems, regardless of the OS that is being used. Tightening the security of your network may include the use of routers, firewalls, and VPNs in accordance with industry-accepted practices.

Fundamentally, no operating system is inherently immune to malicious applications (intentional or unintentional). Avaya continually assesses its software against new threats, defenses, upgrades, and patches, and also reviews its architecture to find ways to improve its resilience to security threats.

Summary
Although no operating system is inherently immune to malicious applications, the Oryx Pecos and Unix/Linux operating systems currently distributed by Avaya are immune to Windows-based Code Red, Nimda, and BadTrans viruses.