Root Cause Analysis Report

Prepared For: Affected Customers
Prepared By: Michelle Pooley, Technical Manager

On behalf of CWCS Managed Hosting

Supreme Hosting. Supreme Support.

Incident Description

Servers on our shared infrastructure experienced varying degrees of very high packet loss between 11:20 and 12:45 on the 25th February 2013. Alongside this a small number of dedicated servers also experienced high packet loss between 11:20am and 13:20 on the 25th February 2013.

Type of Investigation Undertaken

The support teams were alerted to the issue immediately by the network monitoring systems, and network engineers were dispatched to the data center to investigate. Packet loss to the shared platforms and a small number of dedicated servers were immediately confirmed, and analysis began on the traffic logs for the perimeter firewalls.

Due to the nature of the congestion, the investigation took some time to complete. Identification of the traffic source IP addresses on the shared platform were identified and blocked, and some minutes later the same was done for the affected dedicated server infrastructure.

Findings

During the troubleshooting process it became apparent that due to the congestion the support team could not reach some of the information needed to securely access the perimeter firewalls, as some of the network routes used by support were also experiencing severe latency. This caused a delay in staff being able to access key systems during a network incident. This will be addressed immediately.

There was also a slight delay in communicating with customers during the incident with regards to updating the status page. In addition the link to the status updates via the support system was not loading; however this has now been rectified.

Positive Features and Good Practice

All of CWCS' technical teams followed the predefined procedures for dealing with such events where alerts are raised for the core network infrastructure.

CWCS always strive to provide a pro-active and swift response to such situations, we are confident that if such a pro-active approach was not taken for this incident there was a real risk of the entire platform being severely degraded for an extended period.

Recommendations and Action Plan

Recommendation	Action	By Whom	Due Date
Measures to be put in place to ensure the support staff have easy but secure access to the perimeter firewalls if primary systems are congested.	Console login policy to be reviewed by the System Admin team.	Technical Manager/System Administrators	Monday 25th Feb 2013
Support processes to be reviewed regarding status page updates and customer communication during network incidents.	Process updates and internal training to be carried out.	Technical Manager/Team Leader	Tues 26th Feb