Threat Update Service* Advisory
August 3, 2012

Purpose: The Corero Security Active Response Team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Ricoh DC FTP Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in Ricoh DC Software DL-10 because it does not properly validate FTP commands. This could allow an attacker to execute arbitrary code on the remote machine by sending very long FTP commands. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Recommended Action: Apply the specified protection pack (or any later one) and ensure the associated rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	SA47912
Advisory	http://secunia.com/advisories/47912
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Ricoh DC Software DL-10 4.x
Corero Products	IPS 5500 4.X and later.
Associated Rule	tln-004003
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” and “Recommended Client Protection” rule sets.

* previously called TopResponse

