Security Advisory 8-19-2011

Vulnerability when Hosting Control Panel end-users are downloading files using the CDP Web Interface.

Severity

R1Soft rates this vulnerability Critical.

Risk Assessment

We have identified a security flaw in Hosting Control Panel end-user file download which may affect CDP Enterprise & Advanced Edition instances in the public environment. The vulnerability allows a control panel end-user to download files outside of their home directory that they do not have privileges to.

Risk Mitigation

You should immediately upgrade to CDP 3.12.3 or later OR disable all configured hosting control panel instances on your CDP Policies. Disabling the configured hosting control panel instances on your CDP Policies will prevent a control panel end-user from exploiting the vulnerability.

Vulnerability

CDP Server Actions:
Login to the CDP Server web interface and to a hosting control panel instance using the credentials of the control panel end-user. Then use the download to zip or tar archive functionality.

Affected CDP Versions:
CDP Enterprise/Advanced Editions: 3.12.0, 3.12.1, 3.12.2

Fix

This issue has been fixed in CDP 3.12.3. Which you can download from the customer download portal http://download.r1soft.com



Important Note
Only the CDP Server needs to be upgraded to 3.12.3 No agent update is required for the fix.
See the release notes.