

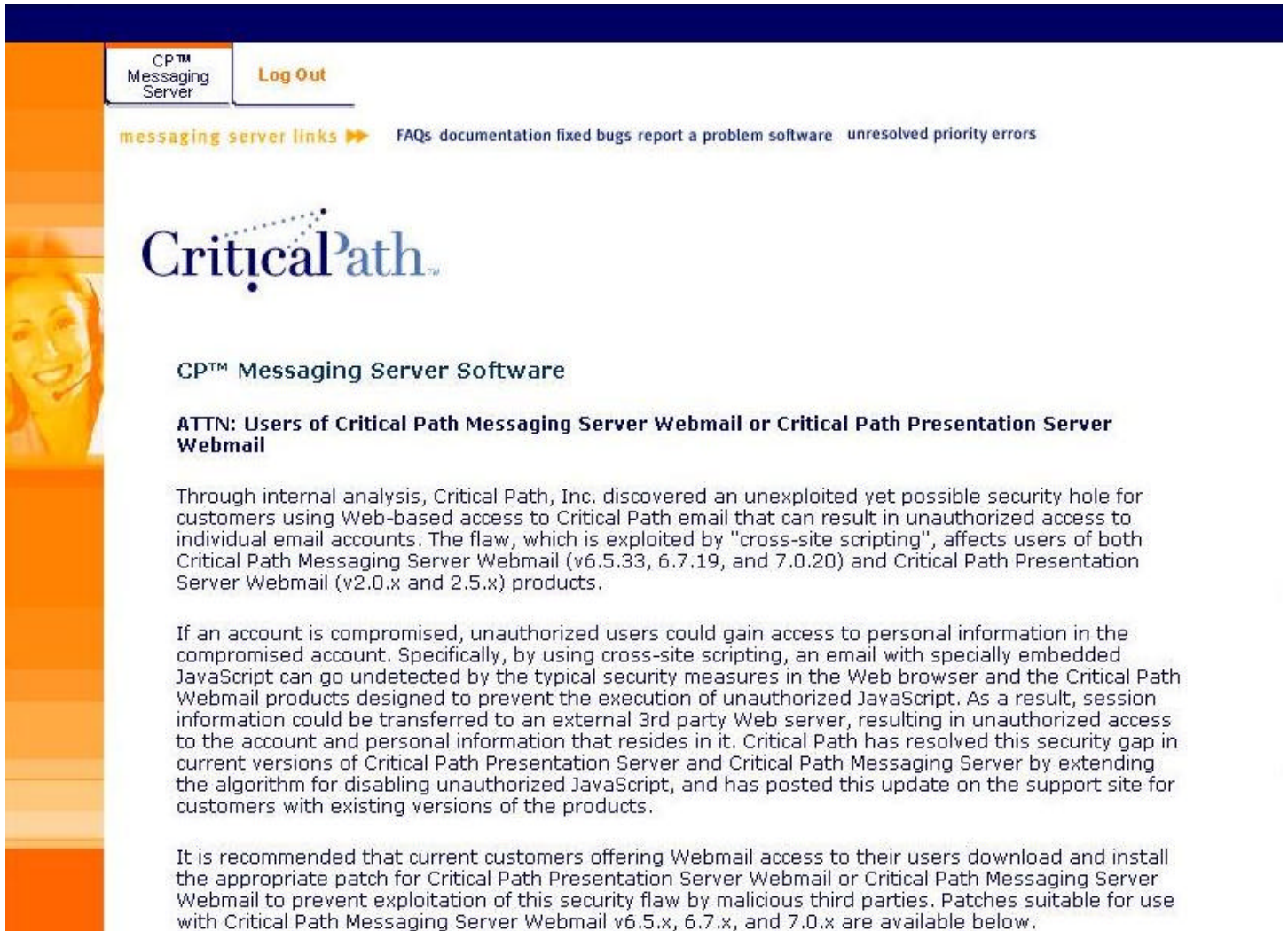


Actualización del microcódigo en el Celerra y aplicación de parche de seguridad en el servicio de Correo Electrónico **Plan de Trabajo**

Actualización del microcódigo en el Celerra y aplicación de parche de seguridad en el Servicio de Correo.

Equipos	Celerra
Objetivos	<ul style="list-style-type: none">• Actualizar el microcódigo del Celerra a la versión 5.1• Aplicar parche de seguridad al CPMS 6.7.19
Justificaciones	<ul style="list-style-type: none">• La actualización del microcódigo del Celerra es un requisito indispensable para el proyecto de replicación del Celerra .• La aplicación del parche es mandatoria para corregir vulnerabilidad reportada por Critical Path.
Tiempo de Ejecución	2 horas
Tiempo de Contingencia	2.5 horas
Fecha Tentativa	10 de Enero de 2003 a las 5:00 a.m.

Aviso recibido de Critical Path referente a la vulnerabilidad detectada en el CPMS 6.7.19



CP™ Messaging Server [Log Out](#)

[messaging server links](#) ► [FAQs](#) [documentation](#) [fixed bugs](#) [report a problem](#) [software](#) [unresolved](#) [priority errors](#)

CriticalPath™

CP™ Messaging Server Software

ATTN: Users of Critical Path Messaging Server Webmail or Critical Path Presentation Server Webmail

Through internal analysis, Critical Path, Inc. discovered an unexploited yet possible security hole for customers using Web-based access to Critical Path email that can result in unauthorized access to individual email accounts. The flaw, which is exploited by "cross-site scripting", affects users of both Critical Path Messaging Server Webmail (v6.5.33, 6.7.19, and 7.0.20) and Critical Path Presentation Server Webmail (v2.0.x and 2.5.x) products.

If an account is compromised, unauthorized users could gain access to personal information in the compromised account. Specifically, by using cross-site scripting, an email with specially embedded JavaScript can go undetected by the typical security measures in the Web browser and the Critical Path Webmail products designed to prevent the execution of unauthorized JavaScript. As a result, session information could be transferred to an external 3rd party Web server, resulting in unauthorized access to the account and personal information that resides in it. Critical Path has resolved this security gap in current versions of Critical Path Presentation Server and Critical Path Messaging Server by extending the algorithm for disabling unauthorized JavaScript, and has posted this update on the support site for customers with existing versions of the products.

It is recommended that current customers offering Webmail access to their users download and install the appropriate patch for Critical Path Presentation Server Webmail or Critical Path Messaging Server Webmail to prevent exploitation of this security flaw by malicious third parties. Patches suitable for use with Critical Path Messaging Server Webmail v6.5.x, 6.7.x, and 7.0.x are available below.

Plan de Trabajo

Estado Actual

- La versión de microcódigo del Celerra es 4.2
- Los servidores de correo tienen CP Messaging Server 6.7.19.

Estado Final

- La versión de microcódigo del Celerra será 5.1
- Los servidores de correo tendrán CP Messaging Server 6.7.19.1

Respaldo

Previo al mantenimiento se realizará un respaldo de los binarios de cada uno de los servidores del cluster de correo.

A continuación se detalla las actividades a realizar, el orden en que deben efectuarse, la entidad responsable de realizarlas y el tiempo invertido.

Nota: Las actividades descritas en un mismo renglón se ejecutarán en paralelo.

TEC DDT	EMC	Tiempo invertido
Dar de baja el servicio de correo en los MTAs y después en el servidor de configuración activo (mailconf2.itesm.mx).		10 minutos
Desmontar los shares del Celerra en los servidores de correo.		5 minutos
Aplicar el parche al CPMS en los servidores de correo.	Actualizar el microcódigo en el Control Station.	25 minutos (*)
	Aplicar el microcódigo en los data movers.	60 minutos
Redistribuir los shares dentro de los data movers del Celerra.		5 minutos
Montar los shares del Celerra en los servidores de correo.		5 minutos
Iniciar el servicio de correo en el servidor de configuración y después en los MTAs.		5 minutos
Realizar pruebas de envío y recepción de correo		5 minutos

(*) En caso de que ocurra una falla en la actualización del microcódigo en el Control Station, se regresará a la versión 4.2 (Tiempo estimado: 30 minutos).