

ZDI-06-021: WebEx Downloader Plug-in Code Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-07/msg00090.html>

- *From:* zdi-disclosures@xxxxxxxxx
 - *Date:* Thu, 6 Jul 2006 17:05:09 -0700
-

ZDI-06-021: WebEx Downloader Plug-in Code Execution Vulnerability

<http://www.zerodayinitiative.com/advisories/ZDI-06-021.html>

July 6, 2006

-- CVE ID:
CVE-2006-3423

-- Affected Vendor:
WebEx Communications

-- Affected Products:
WebEx Downloader Plug-in (tested on v2.0.0.7)

-- TippingPoint(TM) IPS Customer Protection:
TippingPoint IPS customers have been protected against this vulnerability since April 3, 2006 by Digital Vaccine protection filter ID 4274. For further product information on the TippingPoint IPS:

<http://www.tippingpoint.com>

-- Vulnerability Details:
This vulnerability allows attackers to execute arbitrary code on vulnerable installations of the WebEx Downloader Plug-in. Successful exploitation requires that the target user browse to a malicious web page.

The specific flaws exists due to the lack of input validation on various ActiveX/Java control parameters and configuration directives. The "GpcUrlRoot" and "GpcIniFileName" ActiveX/Java control parameters allow an attacker to specify the location of a configuration file containing further control directives. This allows an attacker to transfer arbitrary files and executables to the target. The attacker can then leverage available configuration directives to execute the newly created executables thereby compromising the underlying system.

-- Vendor Response:
WebEx has addressed this issue in the latest release of the Downloader plug-in. More informaton is available from the vendor advisory

ZDI-06-021: WebEx Downloader Plug-in Code Execution Vulnerability

(#WEBX-06-1-1) at:

<http://www.webex.com/lp/security/ActiveAdv.html?TrackID=123456>

— Disclosure Timeline:

2006.04.03 – Digital Vaccine released to TippingPoint customers

2006.04.11 – Vulnerability reported to vendor

2006.07.06 – Coordinated public release of advisory

— Credit:

This vulnerability was discovered by an anonymous researcher.

— About the Zero Day Initiative (ZDI):

Established by TippingPoint, a division of 3Com, The Zero Day Initiative (ZDI) represents a best-of-breed model for rewarding security researchers for responsibly disclosing discovered vulnerabilities.

Researchers interested in getting paid for their security research through the ZDI can find more information and sign-up at:

<http://www.zerodayinitiative.com>

The ZDI is unique in how the acquired vulnerability information is used. 3Com does not re-sell the vulnerability details or any exploit code. Instead, upon notifying the affected product vendor, 3Com provides its customers with zero day protection through its intrusion prevention technology. Explicit details regarding the specifics of the vulnerability are not exposed to any parties until an official vendor patch is publicly available. Furthermore, with the altruistic aim of helping to secure a broader user base, 3Com provides this vulnerability information confidentially to security vendors (including competitors) who have a vulnerability protection or mitigation product.