ERNW Newsletter 10 / Juni 2006

Liebe Partner, liebe Kollegen,

willkommen zur zehnten Ausgabe des ERNW-Newsletters, der sie heute über unser aktuelles Security Advisory informiert.

Die beschriebene Sicherheitslücke

"Buffer Overflow in Algorithmic Researchs PrivateWire Online Registration Facility"

hat unser IT-Security Research-Team unter der Leitung von Michael Thumann aufgedeckt.

Die Aufgabe des ERNW IT-Security Research-Teams ist es, bisher unbekannte Sicherheitsprobleme aufzudecken. Dies können sowohl Sicherheitsprobleme auf konzeptioneller wie auch auf technischer Ebene sein (z.B. Fehlersuche in Software).

Gefundene Probleme werden an die jeweiligen Hersteller kommuniziert und üblicherweise in Kooperation behoben. Sobald eine Lösung für das Problem (z.B. in Form eines Patches) verfügbar ist, wird das Thema entweder in Form eines White-Papers oder als ERNW Security-Advisory veröffentlicht.

Das Research-Team setzt unterschiedlichste Techniken ein um Sicherheitslücken aufzuspüren: von Reverse Engineering über Code Audits bis zur Protokollierung von Netzwerk-Kommunikation oder auch Fault-Injection Techniken.

Die Arbeit des ERNW IT-Security Research-Teams dient sowohl der internen Weiterbildung als auch unseren Kunden, die durch die Ergebnisse dieser Forschungen die allgemeine Sicherheit in der IT weiter verbessern können.

Sollten Sie von der unten genannten Sicherheitslücke betroffen sein stehen wir Ihnen selbstverständlich mit Rat und Tat zur Seite.

ERNW Security Advisory 01-2006:

Buffer Overflow in Algorithmic Researchs PrivateWire Online Registration Facility

Author:
Michael Thumann <mthumann[at]ernw.de>

1. Summary:
The Online Registration Facility of Algorithmic Research PrivateWire VPN Software doesn't do proper bounds checking handling normal GET requests.
Sending an overlong page or script name, it causes a buffer overflow and an attacker can control the EIP to run arbitrary code on the victims machine.

2. Severity : Critical

3. Products affected
All Versions of the PrivateWire Gateway Software up to version 3.7

4. Patch Availability :
A patch is available from the vendor www.arx.com

5. Details
The following request causes PrivateWire to crash:

GET /AAAAAA.....AAAA with 8160 As

6. Solution
Contact the vendor and install the patch.

7. Time-Line
19 Dec 2005: Vulnerability reported to vendor
21 Dec 2005: Telephone conference with vendor
04 Apr 2006: Patch available
26 June 2006: Public Disclosure

8. Disclaimer
The informations in this advisory are provided "AS IS" without warranty of any kind. In no event shall the authors be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages due to the misuse of any information provided in this advisory.

Michael Thumann

ERNW GmbH
Michael Thumann
Senior Security Consultant

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
mthumann@ernw.de
www.ernw.de