# CVE Detail – CVE-2004-0213

Utility Manager in Windows 2000 launches winhlp32.exe while Utility Manager is running with raised privileges, which allows local users to gain system privileges via a "Shatter" style attack that sends a Windows message to cause Utility Manager to launch winhlp32 by directly accessing the context sensitive help and bypassing the GUI, then sending another message to winhlp32 in order to open a user-selected file, a different vulnerability than CVE-2003-0908.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.84109

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-306: Missing Authentication for Critical Function

## CAPEC(s)

* CAPEC-12: Choosing Message Identifier
* CAPEC-166: Force the System to Reset Values
* CAPEC-216: Communication Channel Manipulation
* CAPEC-36: Using Unpublished Interfaces or Functionality
* CAPEC-62: Cross Site Request Forgery

## Affected Products

* cpe:2.3:o:microsoft:windows\_2000:-:sp2:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_2000:-:sp3:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_2000:-:sp4:\*:\*:\*:\*:\*:\*