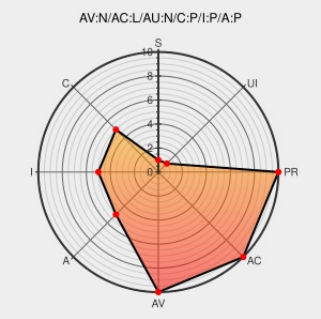
CVE-2014-9707

Published on: 03/31/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9707

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Goahead from Embedthis contain the following vulnerability:

EmbedThis GoAhead 3.0.0 through 3.4.1 does not properly handle path segments starting with a . (dot), which allows remote attackers to conduct directory traversal attacks, cause a denial of service (heap-based buffer overflow and crash), or possibly execute arbitrary code via a crafted URI.

CVE-2014-9707 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20150328 Advisory: CVE-2014-9707: GoAhead Web Server 3.0.
FIX: Dot filename segments permit directory traversal [issue 106] · embedthis/goahead@eed4a7d · GitHub	web.archive.org text/html Inactive Link Not Archived	CONFIRM github.com/embedthis/goahead/commit/eed4a7d177bf94a54c7b06ccce88507fb
URI Parsing Dot Segments · Issue #106 · embedthis/goahead · GitHub	web.archive.org text/html Inactive Link Not Archived	CONFIRM github.com/embedthis/goahead/issues/106
GoAhead 3.4.1 Heap Overflow	Exploit	MISC packetstormsecurity.com/files/131156/GoAhead-3.4.1-Heap-Overflow-

/ Traversal ≈ Packet Storm	packetstormsecurity.com text/html	Traversal.html
Full Disclosure: Advisory: CVE-2014-9707: GoAhead Web Server 3.0.0 - 3.4.1	Exploit seclists.org text/html	FULLDISC 20150328 Advisory: CVE-2014-9707: GoAhead Web Server 3.0.(
GoAhead Web Server Heap Overflow in websNormalizeUriPath() Lets Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1032208

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Embedthis	Goahead	3.0.0	All	All	All
Application	Embedthis	Goahead	3.3.1	All	All	All
Application	Embedthis	Goahead	3.3.2	All	All	All
Application	Embedthis	Goahead	3.3.3	All	All	All
Application	Embedthis	Goahead	3.3.4	All	All	All
Application	Embedthis	Goahead	3.3.5	All	All	All
Application	Embedthis	Goahead	3.3.6	All	All	All
Application	Embedthis	Goahead	3.4.0	All	All	All
Application	Embedthis	Goahead	3.0.0	All	All	All
Application	Embedthis	Goahead	3.3.1	All	All	All
Application	Embedthis	Goahead	3.3.2	All	All	All
Application	Embedthis	Goahead	3.3.3	All	All	All
Application	Embedthis	Goahead	3.3.4	All	All	All
Application	Embedthis	Goahead	3.3.5	All	All	All
Application	Embedthis	Goahead	3.3.6	All	All	All
Application	Embedthis	Goahead	3.4.0	All	All	All

cpe:2.3:a:embedthis:goahead:3.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:embedthis:goahead:3.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:embedthis:goahead:3.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:embedthis:goahead:3.3.3:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.4:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.5:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.6:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.4.0:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.0.0:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.1:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.2:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.3:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.4:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.5:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.3.6:*:*:*:*:*:*:*

cpe:2.3:a:embedthis:goahead:3.4.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→