WEAKNESS

ACCESS AND OUT-OF-BOUNDS WRITE #190, #680

IMPROPER HANDLING OF EXTRA VALUES #231

STRING MANAGEMENT API ABUSE #785, #134, #251

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') #120

SOURCE CODE: Added validation criteria to avoid negative input

if (c->len < 0) {

CVE: Possibly execute arbitrary code via a negative Content-Length HTTP header field... Test with CAPEC 460 (HPP)

Apache Website: buffer overflow can be triggered by receiving an invalid Content-Length header

CONSEQUENCES

WRITE-WHAT-WHERE CONDITION #123

Returns of pointer outside of expected range #466

API ABUSE #227

IMPROPER VALIDATION OF ARRAY INDEX #129, #789

BUFFER COPY WITHOUT CHECKING SIZE OF INPUT

CAN-PRECEDE

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

INCONSISTENCY #130

INDEXABLE-RESOURCE #118

MEMORY-BUFFER #119

STACK-BASED #121

STATIC #129

BUFFER #119

CVE: Allows remote attackers to cause a denial of service (process crash) and possibly execute arbitrary code

Apache Website: cause the Apache child processing the request to crash... This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

RETURN OF POINTER VALUE OUTSIDE OF EXPECTED RANGE #466

ERROR #128

INTEGER OVERFLOW #190, #680

INTEGER UNDERFLOW #191

INTEGER COERCION ERROR #192

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

INCONSISTENCY #130

INDEXABLE-RESOURCE #118

MEMORY-BUFFER #119

STACK-BASED #121

STATIC #129

BUFFER #119

CVE: Heap-based buffer overflow in proxy_util.c for mod_proxy in Apache 1.3.25 to 1.3.31...

Apache Website: A buffer overflow was found in the Apache proxy module, mod_proxy...

Apache Change History: ... buffer overflow in later code...

CONSEQUENCES

WRITE-WHAT-WHERE CONDITION #123

OCCURS-IN

RESOURCE/LOCATION

STACK-BASED #121

STATIC #129

MEMORY-BUFFER #119

BUFFER #119

CVE: Heap-based buffer overflow in proxy_util.c for mod_proxy in Apache 1.3.25 to 1.3.31...

Apache Website: A buffer overflow was found in the Apache proxy module, mod_proxy...

Apache Change History: ... buffer overflow in later code...

CONSEQUENCES

WRITE-WHAT-WHERE CONDITION #123

CAN-PRECEDE

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416

SOFTWARE-FAULT

SIGN ERRORS #194, #195, #196

INCORRECT-BUFFER-SIZE-CALCULATION #131

IMPROPER-INPUT-VALIDATION #20

CWE: ... causes a large amount of data to be copied...

Apache Website: This issue may lead to remote arbitrary code execution on some BSD platforms...

CONSEQUENCES

MISSING INITIALIZATION #456

USE OF DANGEROUS FUNCTIONS #242

IMPROPER USE OF FREED MEMORY #415, #416