



CVE-2021-43618

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-43618
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-15 04:15:00 UTC
Updated	2023-09-29 15:15:00 UTC
Description	GNU Multiple Precision Arithmetic Library (GMP) through 6.2.1 has an mpz/inp_raw.c integer overflow and resultant buffer

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gmplib	Gmp	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference	Source
[SECURITY] [DLA 2837-1] gmp security update	MLIST

Full Disclosure: Re: over 2000 packages depend on abort()ing libgmp	FULLDISC
repo/gmp-6.2: 561a9c25298e	MISC
#994405 - libgmp10:i386: buffer overflow due to integer overflow in mpz/inp_raw.c on 32-bit machines - Debian Bug report logs	MISC
GMP: Buffer Overflow Vulnerability (GLSA 202309-13) — Gentoo security	GENTOO
CVE-2021-43618 GMP Vulnerability in NetApp Products NetApp Product Security	CONFIRM
oss-security - Re: sagemath denial of service with abort() in gmp: overflow in mpz type	MLIST
Segmentation fault with mpz_inp_raw on gcc45	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161093 Oracle Enterprise Linux Security Update for gmp security and enhancement update (ELSA-2023-6661)
178922 Debian Security Update for gmp (DLA 2837-1)
180369 Debian Security Update for gmp (CVE-2021-43618)
198983 Ubuntu Security Notification for GMP Vulnerability (USN-5672-1)
199578 Ubuntu Security Notification for GMP Vulnerability (USN-5672-2)
242306 Red Hat Update for gmp (RHSA-2023:6661)
243028 Red Hat Update for gmp (RHSA-2024:1102)
296099 Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)
354344 Amazon Linux Security Advisory for gmp : ALAS2022-2022-177
354441 Amazon Linux Security Advisory for gmp : ALAS2022-2022-135
355201 Amazon Linux Security Advisory for gmp : ALAS2023-2023-033
356754 Amazon Linux Security Advisory for gmp : ALAS2-2023-2369
500227 Alpine Linux Security Update for gmp
503972 Alpine Linux Security Update for gmp
591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
671251 EulerOS Security Update for gmp (EulerOS-SA-2022-1165)
671278 EulerOS Security Update for gmp (EulerOS-SA-2022-1241)
671302 EulerOS Security Update for gmp (EulerOS-SA-2022-1253)

671339 EulerOS Security Update for gmp (EulerOS-SA-2022-1268)
671360 EulerOS Security Update for gmp (EulerOS-SA-2022-1304)
671365 EulerOS Security Update for gmp (EulerOS-SA-2022-1288)
710756 Gentoo Linux GMP Buffer Overflow Vulnerability (GLSA 202309-13)
751438 SUSE Enterprise Linux Security Update for gmp (SUSE-SU-2021:3878-1)
751455 OpenSUSE Security Update for gmp (openSUSE-SU-2021:3946-1)
751512 OpenSUSE Security Update for gmp (openSUSE-SU-2021:1569-1)
900403 Common Base Linux Mariner (CBL-Mariner) Security Update for gmp (6224)
900881 Common Base Linux Mariner (CBL-Mariner) Security Update for gmp (6444-1)
941374 AlmaLinux Security Update for gmp (ALSA-2023:6661)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)