



Security vulnerabilities (formerly scanner results)



[https://kb.netapp.com/Advice_and_Troubleshooting/Miscellaneous/Security_vulnerabilities_\(formerly_s...](https://kb.netapp.com/Advice_and_Troubleshooting/Miscellaneous/Security_vulnerabilities_(formerly_s...)

Updated: Sun, 11 Jul 2021 11:16:37 GMT

Applies to

Scanner Reports

Answer

Security vulnerabilities (formerly scanner results)

- NetApp takes the security of our products very seriously and is committed to resolving vulnerabilities to meet the needs of our users and the broader technology community.
- As a result of a continually changing threat landscape, NetApp is updating its Product Security Vulnerability Handling and Response Policy.
- NetApp has stopped maintaining the static tables that previously existed on the Scanner Results page.

- Recognizing that users are still interested in information related to potential security vulnerabilities, Common Vulnerability Exposure (CVE) identifiers are searchable in our Bug Tools, Knowledgebase, and [Support](#) sites.
- Our current Security policy is available for review on the NetApp Security landing page: <https://security.netapp.com/>

Current Advisory and Notice Documents

- This page will not be updated for new CVEs.
- Security advisories for announced vulnerabilities can be located here: <https://security.netapp.com/advisory/>
- The [Support](#) and [Security Advisory](#) sites should become the first stop when searching for CVEs impacting NetApp products.
- The following are tables that can help you understand legacy security vulnerabilities related to NetApp products that third-party security scanners might report.
- TABLE A describes CVEs that identify security vulnerabilities applicable to a NetApp product.
- TABLE B describes CVEs that identify security vulnerabilities that might be reported by vulnerability scanners.
- These vulnerabilities constitute 'false positives' reported by vulnerability scanners for user-shipped releases and thus are not believed to represent security exposures for the NetApp products.
- The columns display the CVE number and the NetApp bug tracking number (referred to as a tracking ID on other security pages) where possible, or a title where a bug tracking number is not available.
- It is strongly recommended that end users implement layers of security following security best-practices, including running antivirus tools on the data.
- NetApp storage systems function like file systems to any attached clients.
- While NetApp products might not propagate a given issue, the files and other data objects stored on a NetApp storage system can still be affected by an infected client.

TABLE A: Applicable CVEs

- The listed CVEs might have been applicable to at least one release of Data ONTAP.
- The Public Report for the provided bug tracking number will show the first 'fixed release' when the suspected vulnerability was remediated as well as the subsequent releases that are not subject to the identified vulnerability.

Data ONTAP

CVE	Bug ID
CVE-2005-2969	172506

CVE-2006-4339	267478
CVE-2008-5077	369977
CVE-2008-4609	380197
CVE-2009-3555	386217
CVE-2009-4146, CVE-2009-4147	390420
CVE-2009-3563	394167
CVE-2004-2761	397514
CVE-2008-5161	424122
CVE-2006-0225	457316
CVE-2004-0230	489610
CVE-1999-0524	531251
CVE-2011-3210	536724
CVE-2007-1536	573253
CVE-2007-3798	573282
CVE-2008-3890	573287

CVE-2006-7243, CVE-2010-1128, CVE-2010-1129, CVE-2010-1130, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709, CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE-2010-4645, CVE-2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0421, CVE-2011-0708, CVE-2011-0753, CVE-2011-0754, CVE-2011-0755, CVE-2011-1092, CVE-2011-1148, CVE-2011-1153, CVE-2011-1464, CVE-2011-1466, CVE-2011-1467, CVE-2011-1468, CVE-2011-1469, CVE-2011-1470, CVE-2011-1657, CVE-2011-1938, CVE-2011-2202, CVE-2011-2483, CVE-2011-3182, CVE-2011-3267, CVE-2011-3268, CVE-2011-4566, CVE-2012-0057, CVE-2012-0781, CVE-2012-0788, CVE-2012-0789, CVE-2011-4885, CVE-2012-3365, CVE-2012-2688, CVE-2012-1823, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-1917, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3062, CVE-2010-3063, CVE-2010-3064, CVE-2010-3065	578043
CVE-2006-5794	578973
CVE-2012-2110	602118
CVE-2012-1165	622256
CVE-2013-0169, CVE-2013-0166, CVE-2012-2333, CVE-2012-2131, CVE-2012-2110, CVE-2012-0884, CVE-2012-0050, CVE-2011-4619, CVE-2011-4577, CVE-2011-4576, CVE-2011-4109, CVE-2011-4108, CVE-2011-0014, CVE-2010-4252, CVE-2010-4180, CVE-2010-3864, CVE-2010-2939, CVE-2010-0742	677047
CVE-2005-2969	698797
CVE-2011-1473	707019

Management Tools and Client Products

CVE	Bug ID
-----	--------

CVE-2004-0942, CVE-2005-2728	247972
CVE-2007-6203	275836
CVE-2009-3555	481527
CVE-2009-3720, CVE-2009-3560, CVE-2010-1623, CVE-2010-2068, CVE-2010-1452, CVE-2010-0425, CVE-2010-0434, CVE-2010-0408, CVE-2009-3094, CVE-2009-3095, CVE-2009-2699, CVE-2009-2412, CVE-2009-1890, CVE-2009-1191, CVE-2009-1891, CVE-2009-1195, CVE-2008-0456, CVE-2009-1956, CVE-2009-1955, CVE-2009-0023	487642
CVE-2010-4476	494500
CVE-2010-4476	494539
CVE-2010-4476	497845
CVE-2010-4476	500839
CVE-2011-0419, CVE-2011-3192, CVE-2011-3348	532848
CVE-2010-4476	586066
CVE-2012-0021, CVE-2011-3368, CVE-2011-3607, CVE-2011-4317, CVE-2012-0031, CVE-2012-0053, CVE-2011-3192, CVE-2009-0023, CVE-2009-1191, CVE-2009-1195, CVE-2009-1891, CVE-2009-1955, CVE-2009-1956, CVE-2009-1890	590689
CVE-2012-0884	597187
CVE-2012-2131	602441

CVE-2012-1165	641032
CVE-2013-3320	654355
CVE-2013-3321	654357
CVE-2013-3322	654360
CVE-2013-0169	677043
CVE-2014-0098, CVE-2013-6438, CVE-2013-4365, CVE-2013-2249, CVE-2013-2765, CVE-2013-1896, CVE-2013-1862, CVE-2012-3499, CVE-2012-4558, CVE-2012-0883, CVE-2012-2687, CVE-2011-3368, CVE-2011-3607, CVE-2011-4317, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053, CVE-2012-4557, CVE-2011-3348, CVE-2011-3192	758123

TABLE B: False-Positive and Never Applicable CVEs

These CVEs are either 'false positives' reported by vulnerability scanners or were never applicable to user-shipping versions of the respective NetApp products.

Data ONTAP

CVE	Bug ID
CVE-2000-0666	706057
CVE-2000-0800	746293
CVE-2005-2798	235607
CVE-2006-0225	415006

CVE-2006-0900	422926
CVE-2004-0175	424117
CVE-2007-4752	424118
CVE-2008-1483	424119
CVE-2008-3259	424121
CVE-2003-0190	424123
CVE-2009-1890	440854
CVE-2010-0434	440857
CVE-2010-3069	447837
CVE-2005-1849	467614
CVE-2011-0546	509858
CVE-2012-0027, CVE-2011-4577, CVE-2011-4109, CVE-2011-4108	563327
CVE-2012-0050	567553
CVE-2003-1562	568939
CVE-2006-0883	568947

CVE-2011-4313	574704
CVE-2011-1910	574731
CVE-2006-4925	578971
CVE-1999-0625	597184
CVE-2012-1182	599236
CVE-2012-2110	600349
CVE-2008-1657	603940
CVE-2011-4327	634723
CVE-2013-2686, CVE-2013-0169	677042
CVE-2013-0166	685330
CVE-2004-0079	698728
CVE-2004-0112	698791
CVE-2004-0975	698792
CVE-2008-0891	698802
CVE-2009-0590	698808

CVE-2009-0591	698810
CVE-2009-3245	698837
CVE-2009-4355	698842
CVE-2010-0433	698847
CVE-2010-0742	698849
CVE-2010-1633	698850
CVE-2011-3207	698858
CVE-2010-1452	699180
CVE-2010-2068	699182
CVE-2007-2243	751099
CVE-2000-1200	790912
CVE-2006-5794	824674
CVE-2006-4925	824687

Management Tools and Client Products

CVE	Bug ID
-----	--------

CVE-2011-0419	530008
CVE-2012-3499, CVE-2012-4558	701918

Disclaimer

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Additional Information

additionalInformation_text