



White Paper

NetApp Product Vulnerability, Assessment, and Reporting Policies

V. 1.0

July 2025 | WP-7376

Abstract

This white paper outlines the basic tenants of product vulnerability, assessment, and reporting policies in the NetApp® portfolio.

Product vulnerability, assessment, and reporting

NetApp standard procedures include the implementation of secure design principles, developer training, and extensive testing programs. When product vulnerabilities are identified, we follow a standard process to address vulnerabilities and notify our customers.

- **Vulnerability report received.** NetApp encourages customers and researchers to use PGP-encrypted emails to transmit confidential details to our Vulnerability Response Team (PSIRT). NetApp will investigate a suspected vulnerability in our products and confirm receipt of the vulnerability report within seven business days.
- **Verification.** NetApp PSIRT engineers will verify the vulnerability and provide assessment within the Common Vulnerability Scoring System (CVSS) framework.
- **Resolution development.** NetApp strives to deliver critical fixes and mitigations to the customer base as rapidly as our stringent quality-control standards allow; testing and verification is often a time-intensive process.
- **Notification.** NetApp will disclose the minimum amount of information required for a customer to assess the impact of a vulnerability in their environment, as well as any steps required to mitigate the threat. NetApp does not intend to provide details that could enable a malicious actor to develop an exploit.
- **Attribution.** NetApp will credit the external vulnerability discoverer(s) in the advisory if they have provided explicit consent to be identified, and if they provide NetApp the opportunity to remediate and notify our customer base prior to making the vulnerability public.

NetApp scores security vulnerabilities and prioritizes responses according to industry standards.

To standardize the description of each public vulnerability, NetApp security advisories reference a CVE ID. NetApp uses version 4.0 of the CVSS to determine vulnerability priority and notification strategy.

Our security advisories include the NetApp determined base vulnerability score. We encourage customers using CVSS for vulnerability classification and management to compute their own temporal and environmental scores to take full advantage of the CVSS metrics.

Standard delivery methods for NetApp security information include the following:

- **Security advisory.** Provides information regarding security vulnerabilities that might affect NetApp products and require an upgrade, patch, or direct customer action to remediate. NetApp security advisories are listed on the security.netapp.com site.
- **Security bulletin.** Used when a third party makes an unconfirmed public statement about a perceived NetApp product vulnerability, or NetApp products are unofficially implicated in security incidents.
- **Security bug report.** Provides information about low-severity security flaws or false positive security vulnerabilities and is available via [Bugs Online](#) (requires login).

Read more about CVE IDs at [CVE.org](https://cve.org).

For more information about CVSS, visit the FIRST.org/cvss website.

In addition, NetApp's adherence to standards and participation in standards bodies shows our commitment to security best practices. The following industry standards and mandates guide the handling of product vulnerabilities at NetApp and the disclosure of vulnerabilities to our customers and the broader technology community.

- **National Infrastructure Advisory Council (NIAC) Vulnerability Disclosure Framework:**
Guidelines for disclosing and managing vulnerability
- **ISO/IEC29147:2018:** Information technology; security techniques; vulnerability disclosure
- **ISO/IEC30111:2019:** Information technology; security techniques; vulnerability handling processes

NetApp currently participates in the following security communities:

- [FIRST](#) — Forum of Incident Response and Security Teams
- [BSIMM](#) — Building Security In Maturity Model

NetApp has been a technology solutions supplier to the Department of Defense and intelligence community for more than 30 years. We continue to drive a comprehensive data management posture from the tactical edge to the data center core, and now to the cloud.

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright information

Copyright © 2025 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data—Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.