NetWitness® Platform XDR

NetWitness Security Fixes & SLO

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

July, 2023

About CVE Score and NetWitness Score

You can learn how NetWitness Product Security Team uses a new internal vulnerability scoring method called NWSS (NetWitness Security Score). Using NWSS, the NetWitness Product Security team assesses the vulnerability's actual severity score defined within the scope of NetWitness.

NWSS is calculated based on the CVSS 3.1 scoring system. These details are being tracked in corporate defect tracking system (Jira).

Scoring is based on CVE score and NWSS (NetWitness Score):

- Score > = 9.0 = Critical
- Score > = 7.0 & < = 8.9 = Major
- Score > = 4.0 & < = 6.9 = Moderate
- Score < = 3.9 = Minor

Service Level Objective (SLO)

The Service Level Objective for Common Vulnerabilities and Exposures (CVE) are listed in this section. NetWitness shall use commercially reasonable efforts to roll out a fix within the period specified:

CVE Status	Duration
Critical	30 days
Major	60 days
Moderate	120 days
Minor	120 days

NetWitness Releases and CVEs

The following table provides the list of NetWitness Platform XDR releases and details of CVEs addressed.

Fixed in Version	Security Fixes
12.3	Critical: CVE-2022-39135, CVE-2020-26137, CVE-2021-33503, CVE-2019-11324, CVE-2018-20060, CVE-2023-20873, CVE-2023-20862, CVE-2022-36944, CVE-2022-22965, CVE-2022-34169, CVE-2022-22980, CVE-2019-11236 Major: CVE-2023-1393, CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, CVE-2023-21968, CVE-2022-36364, CVE-2023-1370, CVE-2022-45143, CVE-2022-42252, CVE-2021-46877, CVE-2022-42004, CVE-2022-42003, CVE-2020-36518, CVE-2022-23437, CVE-2012-0881, CVE-2013-4002, CVE-2009-2625, CVE-2023-25194, CVE-2023-24998, CVE-2022-41966, CVE-2022-40152, CVE-2022-40151, CVE-2019-10172, CVE-2022-25647, CVE-2022-3171, CVE-2016-5017, CVE-2020-10663, CVE-2022-29885, CVE-2018-1320, CVE-2020-13949, CVE-2019-0205, CVE-2019-0231, CVE-2015-3250, CVE-2021-35517, CVE-2021-36090, CVE-2021-35515, CVE-2021-40829, CVE-2021-40828, CVE-2021-40830, CVE-2022-41881, CVE-2022-41915, CVE-2022-25647, CVE-2022-22978 Moderate & Minor: CVE-2022-38023, CVE-2023-0767, CVE-2023-0286, CVE-2023-0494, CVE-2022-37434, CVE-2022-42703, CVE-2022-4378, CVE-2023-28708, CVE-2021-22569, CVE-2018-1288, CVE-2022-22976
12.2.0.1	Critical: Major: CVE-2022-2132, CVE-2023-21930 Moderate & Minor: CVE-2023-21954, CVE-2023-21939, CVE-2023-21967, CVE-2023-21937, CVE-2023-21938, CVE-2023-21968

12.2	Critical: CVE-2021-42740, CVE-2022-29078, CVE-2022-39353, CVE-2021-23436 Major: CVE-2022-4283, CVE-2022-46340, CVE-2022-46341, CVE-2022-46342, CVE-2022-46343, CVE-2022-46344, CVE-2023-22809, CVE-2022-2964, CVE-2022-41741, CVE-2022-41742, CVE-2022-22950 Moderate & Minor: CVE-2023-21835, CVE-2023-21843, CVE-2023-21830, CVE-2021-25220, CVE-2022-2795, CVE-2021-26401, CVE-2022-21549
12.1.1	Critical: Major: CVE-2022-42898, CVE-2022-3550, CVE-2022-41974 Moderate & Minor: CVE-2022-3551
11.7.3	Critical: Major: CVE-2022-4378, CVE-2022-37434, CVE-2023-0494, CVE-2022-22934, CVE-2022-22936, CVE-2022-22941, CVE-2023-0767, CVE-2023-0286 Moderate & Minor: CVE-2022-42703, CVE-2022-22935
11.7.2	Critical: Major: CVE-2022-38177, CVE-2022-38178, CVE-2022-40674 Moderate & Minor: CVE-2022-21626, CVE-2022-21628, CVE-2022-21619, CVE-2022-21624, CVE-2022-21618, CVE-2022-39399
12.1.0.1	Critical: CVE-2022-2526 Major: CVE-2022-31676, CVE-2022-29154 Moderate & Minor: CVE-2022-21123, CVE-2022-21125, CVE-2022-21166
12.1	Critical: CVE-2021-22930, Major: CVE-2022-1729, CVE-2022-1966, CVE-2022-32250, CVE-2022-1271, CVE-2022-1552, CVE-2022-34169, CVE-2022-21449, Moderate & Minor: CVE-2020-26116, CVE-2020-26137, CVE-2021-3177, CVE-2022-21540, CVE-2022-21541, CVE-2021-42550, CVE-2021-22150, CVE-2021-22151, CVE-2021-3672, CVE-2021-22931,

	CVE-2021-22939
11.7.1.2	Critical: CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-23852, CVE-2022-25235, CVE-2022-25236, CVE-2022-25315 Major: CVE-2022-0492, CVE-2022-21476, CVE-2021-45960, CVE-2021-46143, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-0778, CVE-2022-22720, CVE-2022-24903, CVE-2022-1271, CVE-2021-31607, CVE-2021-21996 (Fixed or Mitigated) Moderate & Minor: CVE-2022-21426, CVE-2022-21434, CVE-2022-21443, CVE-2022-21496, CVE-2021-22004
12.0	Critical: CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-23852, CVE-2022-25235, CVE-2022-25236, CVE-2022-25315 Major: CVE-2022-0492, CVE-2022-21476, CVE-2021-45960, CVE-2021-46143, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-0778, CVE-2022-22720, CVE-2022-24903, CVE-2022-1271, CVE-2021-31607, CVE-2021-21996 (Fixed or Mitigated) Moderate & Minor: CVE-2022-21426, CVE-2022-21434, CVE-2022-21443, CVE-2022-21496, CVE-2021-22004