DELLTechnologies Avamar Server Avamar Platform OS Security Patch Rollup User Guide

Contents

DELLTechnologies Avamar Server Avamar Platform OS Security Patch Rollup

Product Information

Specifications

- Product Name: Dell Avamar Platform OS Security Patch Rollup
- Version: 2024R1

- Manufacturer: Dell Inc.
- Supported Products:
  - Avamar server
  - Avamar combined proxy
  - Avamar Virtual Edition (AVE)
  - Avamar Data Store (ADS)
  - Avamar NDMP accelerator node
  - NetWorker Virtual Edition (NVE)
  - PowerProtect DP Series Appliance/Integrated Data Protection Appliance (IDPA)
- Third-party Components Updated:
  - Java Runtime Environment (JRE)
  - Apache Tomcat
  - BSAFE OwB FIPS package

Product Usage Instructions

- If required, follow these steps to free space on the server's /boot volume when applying the OS security patch rollup on ADS.

NOTE: Ensure all nodes in a multi-node server have the required free space on the /boot volume.

FAQ

- **Q:** How much free space is required on the /boot volume when applying the Security Rollup?
- **A:** The required free space on the /boot volume is 80MB when manually applying the Security Rollup. When applying via Avinstaller, the required amount may differ based on the rollup version. Refer to the documentation for specific requirements.
- **Q:** Which products are supported by this OS Security Patch Rollup?
- **A:** This rollup applies to Avamar server, Avamar combined proxy, Avamar Virtual Edition (AVE), Avamar Data Store (ADS), Avamar NDMP accelerator node, NetWorker Virtual Edition (NVE), PowerProtect DP Series Appliance/Integrated Data Protection Appliance (IDPA).

These release notes contain supplemental information about the Avamar OS security patch rollup and list the common vulnerabilities and exposures (CVEs) that are addressed in 2024R1. For the list of CVEs that pertain to 2019R4 and earlier OS security patch rollups, see Avamar Platform OS Security Patch Rollup Release Notes. These release notes include the following sections:

Revision history

The following table presents the revision history of this document.
Table 1. Revision history

Revision	Date	Description
01	April, 2024	First release of this document for 2024R1.

Avamar platform OS security patch rollup

The Avamar platform OS security patch rollup automates the steps that are required to apply security and operating system updates that are periodically released between scheduled Avamar server software releases. These release notes provide lists of the common vulnerabilities and exposures (CVEs) addressed by each security patch.
The security patches that are listed in this document apply to the following products:

- Avamar server
- Avamar combined proxy
- Avamar Virtual Edition (AVE)
- Avamar Data Store (ADS)
- Avamar NDMP accelerator node
- NetWorker Virtual Edition (NVE)
- PowerProtect DP Series Appliance/Integrated Data Protection Appliance (IDPA)

The latest Dell Security Advisory (DSA) KB article for these products on the Support site provides the support matrix.
This Avamar platform OS security patch rollup updates the following third-party components also, if present:

- Java Runtime Environment (JRE)
- Apache Tomcat
- BSAFE OwB FIPS package

Clean /boot volume

- If required, perform this procedure to free space on the server's /boot volume when you apply the OS security patch rollup on ADS.

About this task

NOTE: To ensure all the nodes in a multi-node server have the required free space on the /boot volume, perform this procedure on the utility node, all storage nodes, spare nodes, and accelerator nodes (if applicable).
NOTE: When you manually apply the Security Rollup, the required amount of free space on the /boot volume is 80MB.

When you apply rollup via the installer, the required amount of free space on the /boot volume differs between rollup releases.
The following table determines how much free space the rollup requires. Compare this value to the observed free space. When the rollup is applied manually, the required amount of free space on the /boot volume is 80MB for every release.

Table 2. Free space targets

Rollup version	Free space target
2022R1 and later	NA

Steps

Open a command shell and log in by using one of the following methods:

- For a single-node server, log in to the server as admin, and then switch user to root by running su -.
- For a multi-node server, log in to the utility node as admin, and then switch user to root by running su -.
- Check the size and free space on the /boot volume by typing the following command: df -h /boot/

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        98M   13M   81M  14% /boot
```

- Verify whether the volume meets the free space target for this rollup version.
- Check for *-dump files on the /boot volume by typing the following command: ls -l /boot/*kdump
- Information similar to the following is displayed in the command shell:

```
-rw-r--r-- 1 root root 10517730 Aug 1 13:14 /boot/vmlinux-KERNEL_VERSION-kdump
```

- Remove kdump files on the/boot volume by typing the following command: rm /boot/*kdump
- List the installed kernels by typing the following command: rpm -qa |grep kernel-default

```
kernel-default-base-VERSION_NEW
kernel-default-base-VERSION_OLD
kernel-default-VERSION_NEW
kernel-default-VERSION_OLD
```

- Display the running kernel version by typing the following command: uname -a

```
Linux test VERSION_NEW #1 SMP Thu Aug 1 15:34:33 UTC 2019 (47e48a4) x86_64 x86_64 x86_64
GNU/Linux
```

- Identify any old kernels from the list of installed kernels. Exclude the running kernel version.
- If present, remove any old kernels by typing the following command on one line: rpm -ev kernel-default-VERSION_OLD kernel-default-base-VERSION_OLD
- Check the installed and running kernel again for any old kernel files in /boot. If present, remove them manually.
- Check for archived .gz files on the /boot volume by typing the following command: ls -l /boot/*.gz

```
-rw-r--r-- 1 root root   357826 Oct 31  2018 /boot/symvers-VERSION_OLD-default.gz
-rw-r--r-- 1 root root   358659 Aug  1 13:14 /boot/symvers-VERSION_NEW-default.gz
-rw-r--r-- 1 root root 10501442 Oct 31  2018 /boot/vmlinux-VERSION_OLD-default.gz
-rw-r--r-- 1 root root 10517730 Aug  1 13:14 /boot/vmlinux-VERSION_NEW-default.gz
```

- If necessary, remove any archived .gz files on the /boot volume by typing the following command: rm /boot/*.gz
- If the space on the /boot volume is still not enough(less than 80MB)(for manual installation), backup and remove the running kernel: mkdir /usr/local/avamar/var/rollup_bak mv /boot/*VERSION_NEW* /usr/local/avamar/var/rollup_bak

NOTE: After the security rollup installation is complete, do not forget to restore the running kernel files by following step 14.

- Check the size and free space on the /boot volume by typing the following command: df -h /boot/

- For manual installation, after rollup installation is complete, restore the running kernel (if backup up is done in step 12) by typing the following command: mv /usr/local/avamar/var/rollup_bak/*-default /boot rm -r /usr/local/avamar/var/rollup_bak

2024R1 CVEs
This release contains patches for the following CVEs, as indicated by the platform. See the spreadsheet included with each release for CVE details, including applicable packages and RPM files.

SUSE Linux Enterprise Server 12 SP5 CVE list for an Avamar server
The CVEs in this section apply to SLES 12 SP5 on an Avamar server.
Table 3. 2024R1 CVEs for SLES 12 SP5 on an Avamar server

CVE-2007-4559	CVE-2012-4559	CVE-2012-4560	CVE-2012-4561	CVE-2013-0176
CVE-2014-0017	CVE-2014-8132	CVE-2015-20107	CVE-2015-3146	CVE-2015-8325
CVE-2015-8668	CVE-2016-0739	CVE-2016-0777	CVE-2016-0778	CVE-2016-10009
CVE-2016-10010	CVE-2016-10011	CVE-2016-10012	CVE-2016-6210	CVE-2016-6515
CVE-2016-8858	CVE-2017-5849	CVE-2018-10933	CVE-2018-20685	CVE-2019-14889
CVE-2019-17540	CVE-2019-25162	CVE-2019-6109	CVE-2019-6110	CVE-2019-6111
CVE-2020-10735	CVE-2020-16135	CVE-2020-1730	CVE-2020-21679	CVE-2020-27783
CVE-2020-36773	CVE-2020-36777	CVE-2020-36784	CVE-2021-20224	CVE-2021-28041
CVE-2021-28861	CVE-2021-28957	CVE-2021-33631	CVE-2021-3634	CVE-2021-41617
CVE-2021-46906	CVE-2021-46915	CVE-2021-46921	CVE-2021-46924	CVE-2021-46929
CVE-2021-46932	CVE-2021-46953	CVE-2021-46974	CVE-2021-46991	CVE-2021-46992
CVE-2021-47013	CVE-2021-47054	CVE-2021-47076	CVE-2021-47077	CVE-2021-47078
CVE-2022-32545	CVE-2022-32546	CVE-2022-32547	CVE-2022-40899	CVE-2022-44267
CVE-2022-44268	CVE-2022-45061	CVE-2022-4806	CVE-2022-48337	CVE-2022-48339
CVE-2022-48564	CVE-2022-48565	CVE-2022-48566	CVE-2022-48627	CVE-2023-1289
CVE-2023-1667	CVE-2023-2283	CVE-2023-24329	CVE-2023-27043	CVE-2023-28746
CVE-2023-3195	CVE-2023-34151	CVE-2023-35827	CVE-2023-3745	CVE-2023-38408
CVE-2023-38469	CVE-2023-38471	CVE-2023-40217	CVE-2023-40745	CVE-2023-41175
CVE-2023-42465	CVE-2023-45322	CVE-2023-46343	CVE-2023-46838	CVE-2023-47233

CVE-2023-4750	CVE-2023-48231	CVE-2023-48232	CVE-2023-48233	CVE-2023-48234
CVE-2023-48235	CVE-2023-48236	CVE-2023-48237	CVE-2023-48706	CVE-2023-48795
CVE-2023-51042	CVE-2023-51043	CVE-2023-51385	CVE-2023-51780	CVE-2023-51782
CVE-2023-52340	CVE-2023-52356	CVE-2023-52429	CVE-2023-52443	CVE-2023-52445
CVE-2023-52449	CVE-2023-52451	CVE-2023-52464	CVE-2023-52475	CVE-2023-52478
CVE-2023-52482	CVE-2023-52502	CVE-2023-52530	CVE-2023-52531	CVE-2023-52532
CVE-2023-52574	CVE-2023-52597	CVE-2023-52605	CVE-2023-5341	CVE-2023-5388
CVE-2023-5752	CVE-2023-6004	CVE-2023-6040	CVE-2023-6356	CVE-2023-6535
CVE-2023-6536	CVE-2023-6597	CVE-2023-6918	CVE-2024-0340	CVE-2024-0607
CVE-2024-0727	CVE-2024-0775	CVE-2024-0985	CVE-2024-1086	CVE-2024-1151
CVE-2024-20918	CVE-2024-20919	CVE-2024-20921	CVE-2024-20922	CVE-2024-20923
CVE-2024-20925	CVE-2024-20926	CVE-2024-20945	CVE-2024-20952	CVE-2024-22667

CVE-2024-23849	CVE-2024-23851	CVE-2024-25062	CVE-2024-26585	CVE-2024-26595
CVE-2024-26600	CVE-2024-26622			

SUSE Linux Enterprise Server 12 SP5 CVE list for an Avamar combined proxy

The CVEs in this section apply to SLES 12 SP5 on an Avamar combined proxy.

Table 4. 2024R1 CVEs for SLES 12 SP5 on an Avamar combined proxy

CVE-2012-4559	CVE-2012-4560	CVE-2012-4561	CVE-2013-0176	CVE-2014-0017
CVE-2014-8132	CVE-2015-3146	CVE-2015-8325	CVE-2015-8668	CVE-2016-0739
CVE-2016-0777	CVE-2016-0778	CVE-2016-10009	CVE-2016-10010	CVE-2016-10011
CVE-2016-10012	CVE-2016-6210	CVE-2016-6515	CVE-2016-8858	CVE-2017-5849
CVE-2018-10933	CVE-2018-20685	CVE-2019-14889	CVE-2019-25162	CVE-2019-6109
CVE-2019-6110	CVE-2019-6111	CVE-2020-16135	CVE-2020-1730	CVE-2020-36773
CVE-2020-36777	CVE-2020-36784	CVE-2021-28041	CVE-2021-33631	CVE-2021-3634
CVE-2021-41617	CVE-2021-46906	CVE-2021-46915	CVE-2021-46921	CVE-2021-46924
CVE-2021-46929	CVE-2021-46932	CVE-2021-46953	CVE-2021-46974	CVE-2021-46991
CVE-2021-46992	CVE-2021-47013	CVE-2021-47054	CVE-2021-47076	CVE-2021-47077
CVE-2021-47078	CVE-2022-48627	CVE-2023-1667	CVE-2023-22655	CVE-2023-2283
CVE-2023-27043	CVE-2023-28746	CVE-2023-35827	CVE-2023-38408	CVE-2023-38469
CVE-2023-38471	CVE-2023-38575	CVE-2023-39368	CVE-2023-40217	CVE-2023-40745
CVE-2023-41175	CVE-2023-43490	CVE-2023-46343	CVE-2023-46838	CVE-2023-47233
CVE-2023-4750	CVE-2023-48231	CVE-2023-48232	CVE-2023-48233	CVE-2023-48234
CVE-2023-48235	CVE-2023-48236	CVE-2023-48237	CVE-2023-48706	CVE-2023-48795
CVE-2023-51042	CVE-2023-51043	CVE-2023-51385	CVE-2023-51780	CVE-2023-51782
CVE-2023-52340	CVE-2023-52356	CVE-2023-52429	CVE-2023-52443	CVE-2023-52445
CVE-2023-52449	CVE-2023-52451	CVE-2023-52464	CVE-2023-52475	CVE-2023-52478
CVE-2023-52482	CVE-2023-52502	CVE-2023-52530	CVE-2023-52531	CVE-2023-52532
CVE-2023-52574	CVE-2023-52597	CVE-2023-52605	CVE-2023-5752	CVE-2023-6004
CVE-2023-6040	CVE-2023-6356	CVE-2023-6535	CVE-2023-6536	CVE-2023-6597
CVE-2023-6918	CVE-2024-0340	CVE-2024-0607	CVE-2024-0727	CVE-2024-0775
CVE-2024-1086	CVE-2024-1151	CVE-2024-20918	CVE-2024-20919	CVE-2024-20921
CVE-2024-20922	CVE-2024-20923	CVE-2024-20925	CVE-2024-20926	CVE-2024-20945
CVE-2024-20952	CVE-2024-22667	CVE-2024-23849	CVE-2024-23851	CVE-2024-25062
CVE-2024-26585	CVE-2024-26595	CVE-2024-26600	CVE-2024-26622	

SUSE Linux Enterprise Server 12 SP5 CVE list for an NVE
The CVEs in this section apply to SLES 12 SP5 on an NVE.

Table 5. 2024R1 CVEs for SLES 12 SP5 on an NVE

CVE-2012-4559	CVE-2012-4560	CVE-2012-4561	CVE-2013-0176	CVE-2014-0017
CVE-2014-8132	CVE-2015-3146	CVE-2015-8325	CVE-2015-8668	CVE-2016-0739
CVE-2016-0777	CVE-2016-0778	CVE-2016-10009	CVE-2016-10010	CVE-2016-10011
CVE-2016-10012	CVE-2016-6210	CVE-2016-6515	CVE-2016-8858	CVE-2017-5849
CVE-2018-10933	CVE-2018-20685	CVE-2019-14889	CVE-2019-25162	CVE-2019-6109
CVE-2019-6110	CVE-2019-6111	CVE-2020-16135	CVE-2020-1730	CVE-2020-36773
CVE-2020-36777	CVE-2020-36784	CVE-2021-28041	CVE-2021-33631	CVE-2021-3634
CVE-2021-41617	CVE-2021-46906	CVE-2021-46915	CVE-2021-46921	CVE-2021-46924
CVE-2021-46929	CVE-2021-46932	CVE-2021-46953	CVE-2021-46974	CVE-2021-46991
CVE-2021-46992	CVE-2021-47013	CVE-2021-47054	CVE-2021-47076	CVE-2021-47077
CVE-2021-47078	CVE-2022-4806	CVE-2022-48627	CVE-2023-1667	CVE-2023-2283
CVE-2023-27043	CVE-2023-28746	CVE-2023-35827	CVE-2023-38408	CVE-2023-38469
CVE-2023-38471	CVE-2023-40217	CVE-2023-40745	CVE-2023-41175	CVE-2023-42465
CVE-2023-46343	CVE-2023-46838	CVE-2023-47233	CVE-2023-4750	CVE-2023-48231
CVE-2023-48232	CVE-2023-48233	CVE-2023-48234	CVE-2023-48235	CVE-2023-48236
CVE-2023-48237	CVE-2023-48706	CVE-2023-48795	CVE-2023-51042	CVE-2023-51043
CVE-2023-51385	CVE-2023-51780	CVE-2023-51782	CVE-2023-52340	CVE-2023-52356
CVE-2023-52429	CVE-2023-52443	CVE-2023-52445	CVE-2023-52449	CVE-2023-52451
CVE-2023-52464	CVE-2023-52475	CVE-2023-52478	CVE-2023-52482	CVE-2023-52502
CVE-2023-52530	CVE-2023-52531	CVE-2023-52532	CVE-2023-52574	CVE-2023-52597
CVE-2023-52605	CVE-2023-5388	CVE-2023-5752	CVE-2023-6004	CVE-2023-6040
CVE-2023-6356	CVE-2023-6535	CVE-2023-6536	CVE-2023-6597	CVE-2023-6918
CVE-2024-0340	CVE-2024-0607	CVE-2024-0727	CVE-2024-0775	CVE-2024-1086
CVE-2024-1151	CVE-2024-20918	CVE-2024-20919	CVE-2024-20921	CVE-2024-20922
CVE-2024-20923	CVE-2024-20925	CVE-2024-20926	CVE-2024-20945	CVE-2024-20952
CVE-2024-22667	CVE-2024-23849	CVE-2024-23851	CVE-2024-25062	CVE-2024-26585
CVE-2024-26595	CVE-2024-26600	CVE-2024-26622		

SUSE Linux Enterprise Server 12 SP5 CVE list for an NDMP accelerator node

The CVEs in this section apply to SLES 12 SP5 on an NDMP accelerator node.

Table 6. 2024R1 CVEs for SLES 12 SP5 on an NDMP accelerator node

CVE-2012-4559	CVE-2012-4560	CVE-2012-4561	CVE-2013-0176	CVE-2014-0017
CVE-2014-8132	CVE-2015-3146	CVE-2015-8325	CVE-2015-8668	CVE-2016-0739
CVE-2016-0777	CVE-2016-0778	CVE-2016-10009	CVE-2016-10010	CVE-2016-10011
CVE-2016-10012	CVE-2016-6210	CVE-2016-6515	CVE-2016-8858	CVE-2017-5849
CVE-2018-10933	CVE-2018-20685	CVE-2019-14889	CVE-2019-25162	CVE-2019-6109

CVE-2019-6110	CVE-2019-6111	CVE-2020-16135	CVE-2020-1730	CVE-2020-36773
CVE-2020-36777	CVE-2020-36784	CVE-2021-28041	CVE-2021-33631	CVE-2021-3634
CVE-2021-41617	CVE-2021-46906	CVE-2021-46915	CVE-2021-46921	CVE-2021-46924
CVE-2021-46929	CVE-2021-46932	CVE-2021-46953	CVE-2021-46974	CVE-2021-46991
CVE-2021-46992	CVE-2021-47013	CVE-2021-47054	CVE-2021-47076	CVE-2021-47077
CVE-2021-47078	CVE-2022-4806	CVE-2022-48627	CVE-2023-1667	CVE-2023-2283
CVE-2023-27043	CVE-2023-28746	CVE-2023-35827	CVE-2023-38408	CVE-2023-38469
CVE-2023-38471	CVE-2023-40217	CVE-2023-40745	CVE-2023-41175	CVE-2023-42465
CVE-2023-46343	CVE-2023-46838	CVE-2023-47233	CVE-2023-4750	CVE-2023-48231
CVE-2023-48232	CVE-2023-48233	CVE-2023-48234	CVE-2023-48235	CVE-2023-48236
CVE-2023-48237	CVE-2023-48706	CVE-2023-48795	CVE-2023-51042	CVE-2023-51043
CVE-2023-51385	CVE-2023-51780	CVE-2023-51782	CVE-2023-52340	CVE-2023-52356
CVE-2023-52429	CVE-2023-52443	CVE-2023-52445	CVE-2023-52449	CVE-2023-52451
CVE-2023-52464	CVE-2023-52475	CVE-2023-52478	CVE-2023-52482	CVE-2023-52502
CVE-2023-52530	CVE-2023-52531	CVE-2023-52532	CVE-2023-52574	CVE-2023-52597
CVE-2023-52605	CVE-2023-5388	CVE-2023-5752	CVE-2023-6004	CVE-2023-6040
CVE-2023-6356	CVE-2023-6535	CVE-2023-6536	CVE-2023-6597	CVE-2023-6918
CVE-2024-0340	CVE-2024-0607	CVE-2024-0727	CVE-2024-0775	CVE-2024-0985
CVE-2024-1086	CVE-2024-1151	CVE-2024-1441	CVE-2024-20918	CVE-2024-20919
CVE-2024-20921	CVE-2024-20922	CVE-2024-20923	CVE-2024-20925	CVE-2024-20926
CVE-2024-20945	CVE-2024-20952	CVE-2024-22667	CVE-2024-23849	CVE-2024-23851
CVE-2024-2496	CVE-2024-25062	CVE-2024-26585	CVE-2024-26595	CVE-2024-26600
CVE-2024-26622				

SUSE Linux Enterprise Server 12 SP5 CVE list for an ADS Gen5A NDMP accelerator node

The CVEs in this section apply to SLES 12 SP5 on an ADS Gen5A NDMP accelerator node.

Table 7. 2024R1 CVEs for SLES 12 SP5 on an ADS Gen5A NDMP accelerator node

CVE-2015-8325	CVE-2016-0777	CVE-2016-0778	CVE-2016-10009	CVE-2016-10010
CVE-2016-10011	CVE-2016-10012	CVE-2016-6210	CVE-2016-6515	CVE-2016-8858
CVE-2018-20685	CVE-2019-6109	CVE-2019-6110	CVE-2019-6111	CVE-2020-26555
CVE-2021-28041	CVE-2021-33631	CVE-2021-41617	CVE-2022-2586	CVE-2023-0461
CVE-2023-31083	CVE-2023-38408	CVE-2023-39197	CVE-2023-39198	CVE-2023-45863
CVE-2023-45871	CVE-2023-46838	CVE-2023-47233	CVE-2023-48795	CVE-2023-51042
CVE-2023-51043	CVE-2023-51385	CVE-2023-51779	CVE-2023-51780	CVE-2023-51782
CVE-2023-5717	CVE-2023-6040	CVE-2023-6121	CVE-2023-6356	CVE-2023-6535
CVE-2023-6536	CVE-2023-6606	CVE-2023-6610	CVE-2023-6931	CVE-2023-6932

CVE-2024-0340	CVE-2024-0775	CVE-2024-1086	CVE-2024-20918	CVE-2024-20919
CVE-2024-20921	CVE-2024-20922	CVE-2024-20923	CVE-2024-20925	CVE-2024-20926
CVE-2024-20945	CVE-2024-20952			

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.
CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.
WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Documents / Resources

	DELLTechnologies Avamar Server Avamar Platform OS Security Patch Rollup [pdf] User Guide Avamar server, Avamar combined proxy, Avamar Virtual Edition AVE, Avamar Data Store ADS, Avamar NDMP accelerator node, NetWorker Virtual Edition NVE, PowerProtect DP Series Appliance-Integrated Data Protection Appliance IDPA, Avamar Server Avamar Platform OS Security Patch Rollup, Server Avamar Platform OS Security Patch Rollup, Avamar Platform OS Security Patch Rollup, OS Security Patch Rollup, Security Patch Rollup, Patch Rollup

References

- User Manual