Bitdefender

Best For Linux Archived Release Notes

Table of Contents

1. 2022

1.1. Version 7.0.3.2115

Release date:

- Fast ring: 2022.12.12
- Slow ring: 2022.12.15

1.1.1. New Features

- Outbound monitoring is now available for Network Attack Defense on Linux endpoints.

1.1.2. Improvements

- Added support for Oracle Linux 8 and Oracle Linux 9 5.15 kernel versions.
- DNF is now the first choice package manager for YUM based operating systems when installing and updating BEST for Linux.

1.1.3. Resolved Issues

- Reconfigure Client tasks with Match List option selected now properly execute for endpoints with a Linux Relay set as an update location. The tasks used to fail, returning a `no suitable update server found` error.
- The EDR module no longer causes increased CPU usage when enabled.
- Fixed an issue causing endpoints with BEST for Linux installed not to appear in the Active Directory tree.

1.2. Version 7.0.3.2106

Release date:

- Fast ring: 2022.11.21
- Slow ring: 2022.11.21

1.2.1. Improvements

- Security fixes

1.3. Version 7.0.3.2104

Release date:

- Fast ring: 2022.11.16
- Slow ring: 2022.11.17

1.3.1. Improvements

- Added support for upcoming features available with the next major GravityZone release.
- KProbes are now available for Linux kernel 6.0.

- Security fixes.

1.4. Version 7.0.3.2085

Release date:

- Fast ring: 2022.10.13
- Slow ring: 2022.10.17

1.4.1. Improvements

- On demand scans are now available for autofs network shares.
- Network Attack Defense now runs as a separate process. This will considerably improve stability.
- The process exclusions from your GravityZone policies now apply to EDR events from endpoints with BEST for Linux installed.
- You can now define assignment rules based on endpoint hostname.
- Live Search now returns a limited amount of information to GravityZone from endpoints with BEST for Linux deployed. The total number of rows generated by the search is included in the response.

1.4.2. Resolved Issues

- Fixed an issue causing Container Protection to only scan the first two levels of a file path.
- Product updates on SLES 12.5 are no longer failing due to zypper license agreement.
- Product updates now properly ignore global `apt` proxy settings.

1.5. Version 7.0.3.2061

Release date:

- Fast ring: 2022.09.12
- Slow ring: 2022.09.19

1.5.1. Improvements

- Added support for additional Fedora kernels. Learn more

1.5.2. Resolved Issues

- Security fixes

1.6. Version 7.0.3.2050

Release date:

- Fast ring: 2022.08.16
- Slow ring: 2022.08.16

Resolved Issues

- The files used by BEST for Linux when EDR is enabled through AuditD now revert to default when no longer needed. This occurs when EDR is disabled or when kprobes are used instead of AuditD.

1.7. Version 7.0.3.2038

Release date:

- Fast ring: 2022.08.03
- Slow ring: 2022.08.03

Resolved Issues

- Fixed an issue causing security updates to fail and increase CPU usage in certain situations.

1.8. Version 7.0.3.2034

Release date:

- Fast ring: 2022:08.01
- Slow ring: 2022:08.02

> **Important**
> This update includes all improvements and fixes from version 7.0.3.2030 [6] released on fast ring.

Resolved Issues

- Security fixes

1.9. Version 7.0.3.2030

Release date:

- Fast ring: 2022.07.28
- Slow ring:

New Features

- The Network Attack Defense module is now available for Linux. Learn more
- EDR Custom rules are now applicable to endpoints with BEST for Linux v7.

Improvements

- BEST for Linux v7 is now compatible with the following distributions:
  - CBL-Mariner 2
  - Ubuntu 22.04
  - Red Hat Enterprise Linux 9
  - AlmaLinux 9
  - Fedora 36
- Added support for the Amazon Linux 2 5.10.x and 5.15.x kernel versions.
- Antimalware engines are no longer loaded when on-access scanning is disabled. This feature does not apply to endpoints where the Container Protection module is installed.

Resolved Issues

- The Security Telemetry feature now properly displays the connection status to the telemetry servers.
- BEST for Linux no longer causes high CPU usage when EDR is enabled.
- Fixed issue causing servers with BEST for Linux to freeze. This was caused by resetting the firewall while using central scan with a hybrid fallback.
- Using BEST for Linux with AuditD on systems running on Red Hat Enterprise Linux Server 6.7 no longer causes high resource usage.
- Closing BEST for Linux v7 now properly terminates the active instance of the program.
- Fixed issue causing BEST for Linux v7 to gradually increase RAM usage over time.

Known Issues

- Starting or stopping Network Attack Defense will reset all active connection done through ports 21 and 22.

1.10. Version 7.0.3.2004

Release date:

- Fast ring: 2022.05.12
- Slow ring: 2022.05.12

Resolved Issues

- On-Demand scanning tasks with low priority no longer cause high CPU usage.
- Assignment rules based on location now properly apply policies to the target IP addresses.
- Quarantined items are now automatically removed as per the policy configuration.

1.11. Version 7.0.3.1999

Release date:

- Fast ring: 2022.05.09
- Slow ring: 2022.05.10

1.11.1. Improvements

- The **Send feedback regarding security agents' health** and **Use Bitdefender Global Protective Network to enhance protection** policy options now also apply to endpoints with BEST for Linux deployed. You can find the options under **General** > **Settings** > **Options** when editing a policy.
- **EDR Custom Rules** are now applicable on endpoints where BEST for Linux is deployed.

1.11.2. Resolved Issues

- Installing BEST for Linux v7 on an endpoint no longer overwrites the locally configured OSQuery service.
- Deploying BEST for Linux on an Amazon Linux Docker environment no longer causes an increased resource usage.

- Fixed an issue that was affecting the communication between BEST for Linux and GravityZone due to an improper integration with Active Directory.
- Deploying BEST for Linux on an Red Hat Enterprise environment no longer causes increase CPU usage.

1.12. Version 7.0.3.1986

Release date:

- Fast ring: 2022.04.04
- Slow ring: 2022.04.06

> **Important**
> This update includes all improvements and fixes from versions 7.0.3.1982 [8] and 7.0.3.1984 [8] released on fast ring.

1.12.1. Resolved Issues

- Resolved a critical issue occurred after the last product update.

1.13. Version 7.0.3.1984

Release date:

- Fast ring: 2022.03.31
- Slow ring: -

1.13.1. Resolved Issues

- Fixed a configuration problem for BEST Relay.

1.14. Version 7.0.3.1982

Release date:

- Fast ring: 2022.03.31
- Slow ring: -

1.14.1. New Features

- Patch Management now supports Smart Scan on Linux.
- Added support for Investigation packages for both BEST for Linux v7 and SDK.

1.14.2. Improvements

- BEST for Linux is now compatible with Linux Mint and Miracle Linux.
- Deploying or updating BEST for Linux with EDR using Linux AuditD now automatically updates configuration files.
- Added support for the **Shut down computer when scan is finished option** scan option.
- Memory usage has been optimized when using system's AuditD.
- EDR events generation has been optimized.

- Added detection for the exploitation of the CVE-2022-0847 vulnerability.
- Information on errors related to Patch Management is now available here.
- Improved product description in Docker Hub.

1.14.3. Resolved Issues

- BEST for Linux now detects Linux AD integrations.
- Attempting to enable SSL on certain server types no longer causes an indefinite retry loop. This would also cause log files to be flooded with error messages.
- Fixed issue causing high CPU usage on systems with BEST for Linux using AuditD.
- Java applications no longer slow down after installing BEST for Linux on endpoints running on the RHEL 7 and RHEL 8 operating systems.
- Using a script to write files in a high number simultaneously no longer causes high CPU utilization.
- Resolved issue causing high CPU utilization when using EDR.
- **Custom Scan** tasks no longer scan shared file paths when the **Scan network share** option is not selected.
- Fixed issue causing On-Access scans to miss threats during performance tests.
- CIFS and NFS protocols are no longer restricted for systems that use the Fanotify notification system.
- Fixed issue causing On-Demand scan task reports to fail to register in logs.
- On-Demand scan logs from endpoints with BEST for Linux v7 now appear properly in Control Center.

1.14.4. Known Issues

- On-Access scanning does not detect threats in network paths mounted using Amazon EFS.

1.15. Version 7.0.3.1956

Release date:

- Fast ring: 2022.03.10
- Slow ring: 2022.03.10

Improvements

- Reduced memory consumption in certain scenarios where EDR is active.

1.16. Version 7.0.3.1948

Release date:

- Fast ring: 2022.02.17
- Slow ring: 2022.02.21

Improvements

- Optimized the error logging and update mechanisms.

1.17. Version 7.0.3.1942

Release date:

- Fast ring: 2022.02.07
- Slow ring: 2022.02.07

Resolved Issues

- Fixed an issue causing slow product initialization.

1.18. Version 7.0.3.1941

Release date:

- Fast ring: 2022.02.03

Resolved Issues

- Linux machines integrated into Active Directory are now being properly detected and appear under the GravityZone console.
- Applying policies no longer generates unnecessary EDR related events causing high CPU usage. This was occurring due to EDR events remaining active while the EDR Sensor was disabled and Advanced Anti-Exploit remained enabled.
- The `bdsecd` process used for debug logging no longer causes high CPU usage

1.19. Version 6.2.21.212

Release date:

- Fast ring: 2022.04.12
- Slow ring: 2022.04.12

Improvements

- Added support for the automatic migration to version 7.

1.20. Version 6.2.21.173

Release date:

- Fast ring: 2022.01.17
- Slow ring: 2022.01.19

Resolved Issues

- EDR events are now properly received from endpoints communicating through a Relay.

2. 2021

2.1. Version 7.0.3.1927

Release date: 2021.12.24

Resolved Issues

- All events are now being sent to Splunk servers.

Known Issues

- Event submissions to Splunk servers currently fail without a fully signed SSL certificate.

2.2. Version 7.0.3.1922

Release date: 2021.12.16

New Features

- Patch Management is now available for BEST for Linux. You can find a list of compatible operating systems here.

Improvements

- You can now schedule recurring product and security content updates to run on endpoints. You can set the task to run on a specific day of the week or after a certain time has passed since the last occurrence.
- A notification is now sent when a system restart is required. You can choose to immediately restart or postpone the process.
- You can now enable an automatic shutdown or system restart based on specific scenarios such as product update or disinfection.
- The **Restart machine** task is now available for Linux endpoints.
- Antimalware events history is now available locally.

Resolved Issues

- Updating BEST for Linux now properly deletes all previous installation packages present on the endpoint.
- Resolved multiple issues causing the security agent to crash or freeze.
- All scan tasks ran through the Bitdefender User Interface Tool (`bduitool`) now receive unique IDs.

2.3. Version 7.0.3.1903

Release date: 2021.12.01

Improvements

- Product update mechanism via our agent installer has been enhanced.

2.4. Version 7.0.3.1899

Release date:

- Fast ring: 2021.11.23
- Slow ring: 2021.11.25

Improvements

Product

- You can now apply policies based on location assignment rules.
- BEST for Linux v7 is now compatible with the following Linux distributions:
  - Rocky Linux 8.x
  - Pardus 21.0x
  - Alma Linux 8.x
  - Ubuntu 21.04 & 21.10
  - Cloud Linux OS
- BEST for Linux v7 is now compatible with 32-bit operating systems on the following distributions:
  - CentOS 6
  - CentOS 7
  - CentOS 10
  - Debian 11
  - Debian 9
  - Red Hat Enterprise Linux 6
  - Ubuntu 14
  - Ubuntu 16
- BEST for Linux v7 now supports DazukoFS for kernel versions 2.6.32.

> **Note**
> As a result of these improvements, feature parity between versions 6 and 7 has been achieved.

Resolved Issues

Product

- BEST for Linux v7 installer no longer incorrectly reports that there is not enough space on disk when the `/opt/bitdefender-security-tools` file exists.
- Starting an installation of BEST for Linux v7 on an endpoint with an older version of v7 installed no longer returns "The product is already installed".
- Fixed the issue causing increased RAM usage on Ubuntu machines.
- Product updates no longer fail when the Relay URL address has a slash (`/`) at the end.
- Running the `deliverall` command no longer archives the `dnf` folder on machines where BEST for Linux v7 has been updated from an older version.

- Product updates no longer fail on SUSE operating systems.
- Updating BEST for Linux v6 to v7 now properly creates the `/usr/bin/bd symlink` file.

Support Tool

- **Troubleshooting Debug session** tasks no longer remain in an **In progress** state.

Advanced Anti-Exploit

- Alerts are no longer incorrectly triggered for `pkexec` and `policykit` processes.

2.5. Version 7.0.3.1869

Release date: 2021.11.16

Resolved Issues

Product

- Security fixes

2.6. Version 7.0.3.1868

Release date: 2021.11.03

Resolved Issues

Product

- Background periodic clean-up of temporary support files no longer causes Bitdefender systems to crash.

2.7. Version 7.0.3.1862

Release date: 2021.10.28

Resolved Issues

Product

- Security content updates no longer cause scan servers to reload.
- Repeated deployments via Relay on the same endpoint no longer apply the same BEST version. This would occur regardless of the specified deployment settings.
- Resolved an issue causing the Quarantine module to fail clearing file descriptors during scans, resulting in higher resource usage.

Improvements

On-Access

- Files previously confirmed as clean and unmodified are no longer scanned when accessed.

2.8. Version 7.0.3.1850

Release date:

- Fast ring: 2021.10.21

- Slow ring: 2021.10.25

Improvements

Product

- **Support Tool** is now available for BEST for Linux v7.

Container Protection

- **On-Access protection** is now available for Security Container Hosts.
- **Container Protection** is now compatible with OpenShift CRI-O Container Engine.

Resolved Issues

Product

- Installing BEST for Linux on an VM with an RPM-based OS after clearing the `yum` cache no longer fails when no internet access is available.

Known Issues

Product

- During scans, the Quarantine module does not clear file descriptors, resulting in higher resource usage.

2.9. Version 7.0.1.1774

Release date:

- Fast ring: 2021.10.04
- Slow ring: 2021.10.05

Resolved Issues

Product

- (`bduitool`) is now available for BEST for Linux v7.
- Bitdefender user no longer appears in GNOME GUI environments.
- BEST for Linux v7 no longer takes ownership of certain APT files, making software updates to fail.

Known Issues

On-demand

- Changing the system time on an endpoint that has scheduled custom scans causes Bitdefender product to crash.

2.10. Version 7.0.1.1762

Release date: 2021.09.29

Resolved Issues

Product

- Kprobes is no longer failing to load after security content updates.
- Fixed issue causing update tasks run on machines with BEST for Linux v7.0.1.1626 installed to fail despite the console showing the update as successful.

2.11. Version 7.0.1.1754

Release date: 2021.09.23

Improvements

Product

- Logs folder location has been changed from `/tmp` to `/opt/bitdefender-security-tools/var/tmp`.
- Network Isolation tasks now work on endpoints which have a proxy configured.
- Support tool is now available for BEST for Linux v7. It is currently available only from the command line interface.

EDR

- The performance of the incidents sensor has been increased by as much as 30% in certain scenarios.
- Extended the EDR support to Amazon Bottlerocket.

Resolved Issues

Product

- Policies now correctly apply communication settings to endpoints that have been upgraded from BEST for Linux v6 to v7.
- GravityZone now properly detecting new deployments of Patch Management.
- Running a **Reconfigure Client** task now correctly checks available disk space before installing a Relay role. The installation will only begin if sufficient disk space is available.
- Uninstalling BEST for Linux v7 from virtual machines no longer results in a crash in certain situations.
- BEST for Linux v7 now properly updating on all SLES machines.
- Running BEST for Linux installation packages downloaded from a custom host no longer fail.
- BEST for Linux v7 now compatible with machines working with FIPS protocol.
- Fixed issue causing policies not to apply correctly when done through a Relay.
- Security fixes.

Advanced Anti-Exploit

- Custom scan exclusions now properly loading.
- On-Access scans no longer scan removed scan paths specified in your policy settings.
- Added exceptions for alerts related to package managers (apt, yum, dnf).
- Techniques are now properly displayed for corresponding generated events.

Container Protection

- Container logs now properly record Security Container updates.
- Restoring a quarantined file to a container now correctly places the file back on the container instead of the host VM.

- Security Containers now work properly with Bottlerocket OS.

2.12. Version 7.0.1.1725

Release date: 2021.09.09

Resolved Issues

Antimalware

- Security content updates no longer cause On-Demand scans to return no results.

2.13. Version 7.0.1.1713

Release date: 2021.09.07

Improvements

- **Network Isolation** for EDR is now available.

Resolved Issues

Product

- Upgrading BEST for Linux from v6 to v7 no longer causes issue where both BEST versions run on the same endpoint.
- Upgrading BEST for Linux from v6 to v7 no longer causes On-Demand scans to return no results.

Relay role

- The Relay role is now supported again.

Known Issues

- **Network Isolation** disconnects endpoints from the network, causing a loss of connectivity with GravityZone. This issue only occurs for endpoints that use policies with proxy configurations.

  > **Note**
  > To change the proxy settings, go to the **General** > **Communication** policy section and choose another option for **Communications between Endpoints and Relays / GravityZone**.

2.14. Version 7.0.1.1626

Release date: 2021.08.12

Resolved Issues

Product

- Policies applied to Security Containers now function independently of policies applied to the host.
- Enabling On-Access on policies that have already been applied no longer fails to activate the service.

- HTTPS protocol updates no longer fail on certain operating systems.
- Running an **Update client** task for both product and security content no longer fails to perform the security content update.
- Scan reports now show the correct number of scanned files.

2.15. Version 7.0.1.1582

Release date: 2021.08.12

Improvements

Container Protection

- Podman inventory support now available.

Resolved Issues

Product

- Update tasks now show correct status after failing.
- Using On-Access scanning on a Ubuntu container no longer causes Bitdefender services to sometimes crash.
- Issues no longer appear when trying to remove malware from certain archives.

Container Protection

- Container runtime now registers properly in all environments.
- When applying policies to containers, configured actions now apply correctly when malware is detected, including on older kernel versions.
- Kprobes no longer being reloaded when no new updates are available.

2.16. Version 7.0.1.1556

Release date: 2021.08.06

Resolved Issues

Product

- Product updates no longer failing when no update locations are added to the policy you are using.

2.17. Version 7.0.1.1551

Release date: 2021.08.05

Resolved Issues

Product

- Product now correctly showing status for disabled modules.
- Performing a scan task during a security content update no longer causes Bitdefender services to sometimes crash.
- Using a proxy server no longer prevents EDR incidents from being generated.

2.18. Version 7.0.1.1520

Release date: 2021.07.29

BEST for Linux v7 is now available with a new set of features and benefits, including:

Features

- Container Protection – protects both the container host and its running containers.
- A new anti-exploit module.

Benefits And Improvements

- A new architecture, created using Kprobes instead of kernel modules, which eliminates the common delays or the need to sacrifice security when upgrading.
- Greatly expanded platform compatibility to all Enterprise Linux distributions and cloud native Linux distributions.

Known Issues

- Policy per location not supported.
- `Bduitool` not supported.
- Relay role not supported.
- Remote troubleshooting not supported.
- **Has issues** status not being removed properly from endpoints once the issue has been resolved.
- SELinux not supported.
- EDR Isolate action not supported.
- **Shut down computer when scan is finished** option not functioning properly after scan is performed. Endpoints are not being shut down.
- Restart computer task with **Restart now** option enabled not functioning properly. Virtual machines and computers are not being restarted.
- Files in mounted network directories not being scanned through On-Access scanning.
- Machines with 32-bit OS not supported.
- Delay in security content update status change after security update.
- On-Access scanning ignoring file size limitation. All file sizes are scanned.

2.19. Version 6.2.21.171

Release date: 2021.11.16

Resolved Issues

Product

- Security fixes

2.20. Version 6.2.21.170

Release date: 2021.09.28

Improvements

- Prior to each deployment of BEST for Linux v6, endpoints will be checked by the system. If BEST for Linux v7 is already installed, the deployment will not be initiated.

Resolved Issues

- Security fixes.

2.21. Version 6.2.21.169

Release date: 2021.08.18

Resolved Issues

Product

- Endpoints with BEST for Linux v7 now properly update on SUSE systems when using BEST for Linux v6 Update Servers.
- Security Server instances now publishing accordingly on Update Servers that use BEST for Linux v6.

2.22. Version 6.2.21.167

Release date:

- Fast ring: 2021.07.21
- Slow ring: 2021.07.22

New Features And Improvements

- Changes were made to Update Server in preparation for BEST for Linux v7 launch.

> **Note**
> No restart is required.

2.23. Version 6.2.21.165

Release date:

- Fast ring: 2021.07.01
- Slow ring: 2021.07.05

New Features And Improvements

Endpoint Detection and Response (EDR)

- Extended the supported kernels list for the EDR module. For more information, refer to the Endpoint Detection and Response (EDR) and supported Linux kernels section.

2.24. Version 6.2.21.160

Release date:

- Fast Ring: 2021.06.03
- Slow Ring: 2021.06.07

New Features And Improvements

Endpoint Detection and Response (EDR)

- Extended the supported kernels list for the EDR module. The new kernel versions are available here.

Resolved Issues

Endpoint Detection and Response (EDR)

- The EDR module caused intermittent reboots and crashes on endpoints that use the DazukoFS module.

Product

- Security fixes.

2.25. Version 6.2.21.155

Release date:

- Fast Ring: 2021.05.17
- Slow Ring: 2021.05.19

Resolved Issues

Product

- The security agent led to system crashes on Red Hat Enterprise Linux after the update to version 8.3.
- Security fixes.

2.26. Version 6.2.21.141

Release date:

- Fast Ring: 2021.04.15
- Slow Ring: 2021.04.19

New Features And Improvements

Relay

- Added support for the newest update locations necessary for the Security Server update process.

2.27. Version 6.2.21.137

Release date:

- Fast Ring: 2021.03.04
- Slow Ring: 2021.03.08

> **Note**
> This version also includes on slow ring the improvements and fixes delivered with the Bitdefender Endpoint Security Tools versions 6.2.21.135 and 6.2.21.136, released on fast ring.

New Features And Improvements

Endpoint Detection and Response (EDR)

- Extended the supported kernels list for the EDR module. For more information, refer to the Endpoint Detection and Response (EDR) and supported Linux kernels section.

Resolved Issues

Product

- Fixed multiple crashes that affected systems with product version 6.2.21.135, released on fast ring.
- The remote deployment of the security agent failed due to permission issues when non-root credentials were used.

Endpoint Detection and Response (EDR)

- The EDR module caused system crashes when the `kubectl` command was used.

2.28. Version 6.2.21.136

Release date:

- Fast Ring: 2021.02.26
- Slow Ring: -

Resolved Issues

Product

- Fixed multiple crashes that affected systems with product version 6.2.21.135, released on fast ring.

2.29. Version 6.2.21.135

Release date:

- Fast Ring: 2021.02.25
- Slow Ring: -

Resolved Issues

Product

- The remote deployment of the security agent failed due to permission issues when non-root credentials were used.

Endpoint Detection and Response (EDR)

- The EDR module caused system crashes when the `kubectl` command was used.

2.30. Version 6.2.21.133

Release date:

- Fast Ring: 2021.02.03

- Slow Ring: 2021.02.08

New Features And Improvements

Bduitool

- Improved the `bduitool` scan options as follows:
  - The command `bduitool get scantask` now returns a task identifier for each task in the list. The tasks in progress are listed first.
  - Every listed timestamp is now followed by the time zone.

  These improvements do not impact the current system requirements.
  For more information, refer to the Bitdefender Endpoint Security Tools for Linux User's Guide section.

Resolved Issues

Product

- The product led to system crashes after updating to Red Hat Enterprise Linux 8.3.
- A corrupted system configuration file (`/etc/fstab`) prevented successful reboots on Red Hat Enterprise Linux 5 and 6.
- The Bitdefender Crash Handler mechanism caused multiple applications to hang leading the system into an unresponsive state.
- Oracle Linux Server systems with the security agent installed reported errors when elevated commands were run.

3. 2020

3.1. Version 6.2.21.125

Release date:

- Fast Ring: 2020.12.15
- Slow Ring: 2020.12.17

New Features And Improvements

General

- Added improvements for product crash scenarios.

Antimalware

- Added improvements for better resource consumption.

3.1.1. Resolved Issues

Installation

- The security agent failed to install on a Red Hat Enterprise 6.5 Korean system.

Antimalware

- The Antimalware module appeared as disabled in the local interface when the mount point used NFSv4.
- The product caused system crashes on Red Hat Enterprise 8.3.

Endpoint Detection and Response (EDR)

- The security agent consumed a large amount of memory triggering Linux Out Of Memory Killer on some Ubuntu systems.

3.2. Version 6.2.21.108

Release date:

- Fast Ring: 2020.11.17
- Slow Ring: 2020.11.17

New Features And Improvements

General

- Added support for the latest Red Hat Compatible Kernels (RHCK) versions of Oracle Linux 7.

3.3. Version 6.2.21.106

Release date:

- Fast Ring: 2020.11.09

- Slow Ring: 2020.11.11

New Features And Improvements

General

- Added support for upcoming features available with the next GravityZone release.

Antimalware

Improved the Bitdefender User Interface Tool (`bduitool`) as follows:

- A task ID is provided when an On-Demand scan task is initiated. Using this unique identifier you can easily manage tasks and find the necessary information.
- The users can now query the status of previous and current On-Demand scan tasks using a task ID. The result consists of an individual summary for each scan task. The summary includes details like scan type, scanned items, a path to the full report, and others.
- On-Demand scan tasks initiated via `bduitool` now support wildcards that expand the full directory path.

3.4. Version 6.2.21.103

Release date:

- Fast Ring: 2020.09.30
- Slow Ring: 2020.10.05

New Features And Improvements

Relay

- Added support to display the latest security content in the **Repository details** tab, in GravityZone console.

Endpoint Detection and Response (EDR)

- Extended the EDR supported kernels list with version 2.6.32.

Quarantine

- Minor improvements related to backing up quarantined files.

Resolved Issues

Antimalware

- In some cases, start time for **On-Demand** scheduled scan tasks was set to UTC regardless of the local time zone.
- The product failed to apply the option **Copy files to quarantine before applying the disinfect action** enabled in the GravityZone console.

Endpoint Detection and Response (EDR)

- The product returned operating system and EDR commands without logging feature enabled.

- The EDR module caused high latencies on Linux systems such as CentOS 7.6.

Patch Management

- In certain conditions, the Patch Management module failed to download patches properly.

General

- Changing standard umask settings to comply with custom security guidelines caused incorrect product installation.

3.5. Version 6.2.21.97

Release date:

- Fast Ring: 2020.09.10
- Slow Ring: 2020.09.10

Resolved Issues

Relay

- Addressed a vulnerability discovered recently.

3.6. Version 6.2.21.94

Release date:

- Fast Ring: 2020.08.24
- Slow Ring: 2020.08.24

> **Important**
> This version also includes on slow ring the improvements and fixes delivered with the Bitdefender Endpoint Security Tools version 6.2.21.92, released on fast ring.

Resolved Issues

General

- The security agent caused disk space usage on Linux systems.

Antimalware

- The endpoint reported infected files as blocked when the scan action was set to **Take no action**.
- In some cases, suspicious or infected files were reported as deleted instead of unresolved in the **Malware Status** report.

3.7. Version 6.2.21.92

Release date:

- Fast Ring: 2020.08.20
- Slow Ring: 2020.08.24

Resolved Issues

General

- The security agent caused disk space usage on Linux systems.

Antimalware

- The endpoint reported infected files as blocked when the scan action was set to **Take no action**.
- In some cases, suspicious or infected files were reported as deleted instead of unresolved in the **Malware Status** report.

3.8. Version 6.2.21.88

Release date:

- Fast ring: 2020.08.12
- Slow ring: 2020.08.12

Resolved Issues

Antimalware

- The product monitoring mechanism failed to use the **Full Scan** settings to determine the infection status of the endpoint.
- Stopping the Bitdefender services while the product was checking the status of an existing infection caused the loss of some files from the monitoring mechanism.

Known Issues

Antimalware

- The On-Access and On-Demand features may report the same files with different names when HyperDetect is set to **Aggressive** or when the option **Extend reporting on higher levels** is selected. This issue causes the **Malware Status** report to display the files as deleted instead of unresolved.

Version 6.2.21.87

Release date:

- Fast Ring: 2020.07.28
- Slow Ring: 2020.07.29

Resolved Issues

General

- The product caused critical errors (Kernel Panic) on CentOS 7 systems.

Version 6.2.21.84

Release date:

- Fast Ring: 2020.07.08
- Slow Ring: 2020.07.09

New Features And Improvements

General

- Incidents based on the Antimalware On-demand scans are now generated and displayed in the GravityZone Control Center.

Version 6.2.21.79

Release date:

- Fast Ring: 2020.07.01
- Slow Ring: 2020.07.01

Resolved Issues

General

- The security agent caused crashes on CentOS 6.10 systems, after updating to version 6.2.21.76.

Version 6.2.21.76

Release date:

- Fast Ring: 2020.06.29
- Slow Ring: 2020.06.30

New Features And Improvements

General

- Added support for upcoming features available with the next GravityZone release.

Resolved Issues

General

- The endpoint submitted multiple events to GravityZone Control Center, which led to high memory consumption.
- Bitdefender Redline service caused high memory usage on CentOS systems.

Version 6.2.21.74

Release date:

- Fast Ring: 2020.06.25
- Slow Ring: 2020.06.30

New Features And Improvements

General

- Added support for upcoming features available with the next GravityZone release.

EDR

- Improved the EDR incidents detections.

- Extended the supported kernels list for the EDR module.

Resolved Issues

General

- The endpoint submitted multiple events to GravityZone console, which led to high memory consumption.
- Bitdefender Redline service caused high memory usage on CentOS systems.

Version 6.2.21.67

Release date:

- Fast Ring: 2020.06.08
- Slow Ring: 2020.06.08

Resolved Issues

- The security agent failed to detect certain machines joined to Amazon Web Services (AWS) which prevented GravityZone from licensing them.

Version 6.2.21.66

Release date:

- Fast ring: 2020.04.23
- Slow ring: 2020.04.23

Resolved Issues

- The product caused deadlocks on CentOS 7 servers in environments with high volume ICMP events.

Version 6.2.21.64

Release date:

- Fast ring: 2020.04.16
- Slow ring: 2020.04.16

Resolved Issues

- The security content updates did not start automatically on endpoints with 6.2.21.63 product version.

Version 6.2.21.63

Release date:

- Fast ring: 2020.04.06
- Slow ring: 2020.04.08

New Features And Improvements

- Added support for generating incidents on Elite licensed endpoints.
- Introduced Bitdefender Update Daemon (`bdupdated`) as a new update service. The previous service (`bdlived`) has been removed.
- Added support for process kill action on incidents generated by **Incidents Sensor**.
- Improved the scanning mechanism with new built-in Antimalware On-Access and On-Demand exclusions.
- Added support for moving endpoints between companies in GravityZone Control Center.
- Improved the On-Demand scheduler.
- Added support for EDR with a new range of Linux kernel versions, available with the following operating systems:
  - CentOS 6
  - CentOS 7
  - CentOS 8
  - Oracle Linux 6
  - Oracle Linux 7
  - Ubuntu 14.04
  - Ubuntu 16.04
  - Ubuntu 18.04

  For the list of supported kernel versions, refer to the Endpoint protection section.
- New installations and product updates now require minimum free disk space as follows:

Scanning type	AV only	Full options
Local scanning	1600 MB	1600 MB
Hybrid scanning	1100 MB	1100 MB
Centralized scanning	600 MB	600 MB
Local scanning + centralized scanning	1600 MB	1600 MB
Hybrid scanning + centralized scanning	1100 MB	1100 MB

Resolved Issues

- The `bduitool` crashed when used for custom scan on Red Hat Enterprise Linux Server.
- The On-Access module could not detect EICAR files located in an overlay partition, on Ubuntu 18.04.1 LTS.
- Bitdefender Redline service triggered multiple cron failure notifications.
- The Relay communication with endpoints failed with error `1004`.
- The endpoint updated through proxy even if it was not configured in the policy.

Version 6.2.21.53

Release date:

- Fast ring: 2020.02.10
- Slow ring: 2020.02.10

> **Caution**
> This version includes on slow ring all the improvements and fixes delivered with Bitdefender Endpoint Security Tools version 6.2.21.49, released on fast ring.

New Features And Improvements

- Enhanced the scanning engines loading mechanism.

Resolved Issues

- The On-Access scanning module interfered with the software compilation process on Ubuntu 18.04, even when disabled.

Version 6.2.21.49

Release date:

- Fast ring: 2020.01.20
- Slow ring: -

Resolved Issues

- The On-Access scanning module interfered with the software compilation process on Ubuntu 18.04, even when disabled.

4. 2019

Version 6.2.21.46

Release date:

- Fast ring: 2019.12.09
- Slow ring: 2019.12.11

Resolved Issues

- The security agent interfered with the authselect application on certain Linux systems.
- Fixed a product incompatibility that required SELinux to be disabled on Linux systems using Fanotify.

Version 6.2.21.42

Release date:

- Fast ring: 2019.10.30
- Slow ring: 2019.11.04

New Features And Improvements

- Added support for configuring Antimalware exclusions in the GravityZone console by file hash or threat name.
- Added support for configuring Antimalware Process exclusions in GravityZone console for the On-Access module.
- Added support for wildcards when customizing Antimalware On-Access /On-Demand exclusions. Question mark (?) substitutes for one character, whereas asterisk (*) substitutes for any number of characters until the special character(/) is reached.
- The product can now be installed at a configured custom path with the following restrictions:
  - All paths have to start with slash (/) – except `%PROGRAMFILES%`
  - Paths starting with `/tmp` or `/proc` are not accepted
  - Paths that contain a special character ($, !, *, ?, “, ‘, `, ‘\’, %) , including any type of parentheses are not accepted
- The EDR Sensor is now improved to reflect the current status more accurately.

Resolved Issues

- Simultaneous contextual scans with `bduitool` resulted in only one local scanlog.
- Bitdefender Redline service triggered multiple cron failure notifications.
- In certain situations, the On-Access module could not detect specific files on XFS partition.
- The **Contextual Scan** archive limit size configured in the policy did not reflect on the endpoint.

Version 6.2.21.32

Release date:

- Fast ring: 2019.07.25
- Slow ring: 2019.07.25

Resolved Issues

- In a particular case, the On-demand scan tasks did not run when using `bduitool`.

Version 6.2.21.31

Release date:

- Fast ring: 2019.07.03
- Slow ring: 2019.07.03

Resolved Issues

- Addressed a particular scenario causing scanning service crashes.

Version 6.2.21.29

Release date:

- Fast ring: 2019.06.26
- Slow ring: 2019.06.27

> **Caution**
> This version includes on slow ring all the improvements and fixes delivered with Bitdefender Endpoint Security Tools versions 6.2.21.27 and 6.2.21.28 released on fast ring.

New Features And Improvements

- Improved EDR Sensor now reports incidents and suspicious activity to GravityZone.

Resolved Issues

- The EDR module was not licensed when installed via a **Reconfigure** task.
- In certain conditions, the product crashed on Debian 9 after updating the agent to version 6.2.21.27.
- The `bduitool` command returned the exit code 0 for both successful and failed statuses. Now for failed operations the command returns error codes different than 0.
- In a particular case, Ubuntu 18.04 physical machine with the EDR module installed stopped.
- High CPU usage occurred on Debian 9 Relay servers.

Known Issues

- When running `bduitool` get ps command on endpoints with EDR Sensor installed, the feature status is always "Installed", even if the module is disabled or the kernel version is unsupported.

Version 6.2.21.28

Release date:

- Fast ring: 2019.06.25
- Slow ring: -

Resolved Issues

- In certain conditions, the product crashed on Debian 9 after updating the agent to version 6.2.21.27.

Version 6.2.21.27

Release date:

- Fast ring: 2019.06.24
- Slow ring: -

New Features And Improvements

- Improved EDR Sensor now reports incidents and suspicious activity to GravityZone.

Resolved Issues

- The `bduitool` command returned the exit code 0 for both successful and failed statuses. Now for failed operations the command returns error codes different than `0`.
- In a particular case, Ubuntu 18.04 physical machine with the EDR module installed stopped.
- High CPU usage occurred on Debian 9 Relay servers.

Known Issues

- When running `bduitool get ps` command on endpoints with EDR Sensor installed, the feature status is always "Installed", even if the module is disabled or the kernel version is unsupported.

Version 6.2.21.23

Release date:

- Fast ring: 2019.05.02
- Slow ring: 2019.05.02

Resolved Issues

- In a particular scenario, the Relay failed to download product kits, causing deployment issues.

4.1. Version 6.2.21.21

Release date:

- Fast ring: 2019.04.22
- Slow ring: 2019.04.22

> **Caution**
> This version includes on slow ring all the improvements and fixes delivered with Bitdefender Endpoint Security Tools for Windows Legacy version 6.2.21.18, released on fast ring.

New Features And Improvements

- New EDR blocklist capability allows administrators to automatically prevent suspicious files from running based on hash.
- Remote deployment now also works using `sudo` to elevate user with full permissions.

Resolved Issues

- In some situations, the product failed to report FQDN for EDR events.
- In some situations, the endpoint crashed at boot time after installing the agent through DazukoFS.
- **Reconfigure Client** task status remained **In Progress** in GravityZone console once completed on the endpoint.
- High memory usage occurred during on-demand scanning on some Ubuntu 18.04 systems.
- Bitdefender Redline connectivity errors are no longer logged to syslog.

Version 6.2.21.18

Release date:

- Fast ring: 2019.04.09
- Slow ring: -

New Features And Improvements

- New EDR blocklist capability allows administrators to automatically prevent suspicious files from running based on hash.
- Remote deployment now also works using `sudo` to elevate user with full permissions.

Resolved Issues

- In some situations, the endpoint crashed at boot time after installing the agent through DazukoFS.

- **Reconfigure Client** task status remained **In Progress** in GravityZone console once completed.
- High memory usage occurred during On-demand scanning on some Ubuntu 18.04 systems.
- Bitdefender Redline connectivity errors are no longer logged to syslog.

Version 6.2.21.12

Release date:

- Fast ring: 2019.02.14
- Slow ring: 2019.02.18

New Features And Improvements

- Streamlined EDR module installation and update process reducing network traffic.
- New installations and product updates now require kernel version 2.6.32 or higher. Installing on older kernels will fail with error 12.
- New installations and product updates now check for and require minimum free disk space (in addition to existing checks for Relay and Patch Caching Serverroles). Installing on systems with insufficient disk space will fail with error 74. The minimum requirements are as follows:

Scanning type	AV only	AV + EDR
Local scanning	1300 MB	1450 MB
Hybrid scanning	800 MB	950 MB
Centralized scanning	300 MB	450 MB
Local scanning + centralized scanning	1300 MB	1450 MB
Hybrid scanning + centralized scanning	800 MB	950 MB

Resolved Issues

- In some cases, the product blocked logical volumes (LV) mounts when using DazukoFS.
- The product now detects AutoFS mount points to avoid mounting NFS file systems using DazukoFS.
- In certain situations when using **Remote Scan**, **On-demand scanning** caused high memory consumption.
- Other minor improvements and bug fixes.