Truview - 11.3 Release Notes

Contents

1 Truview v11.3 2

1.1 New Features 2
1.2 Components Affected 2
1.3 Installation 2
1.4 Known Issues 3
1.5 Defects Fixed 3
1.6 Security Fixes 4

1 Truview v11.3

TruView is a comprehensive system for enabling the successful delivery of enterprise applications over converged networks. This system provides unique views and a range of ways to analyze application, VoIP, and network performance.

1.1 New Features

- Support TruView Packet Install on legacy TV-4400 hardware.
- Can add/modify/delete apps, sites, and servers using TruView APIs in order to automatically configure the system
- User can authenticate using External Authentication including Active Directory, OpenLDAP and RADIUS
    - LDAP GUI Change - Added Advanced section to hide fields that are often default or rarely modified. Also added support to parse BindDN from users email, username and user groups.
    - SSL + TLS Support for External Authentication - Added ability to support SSL and TLS for External Authentication,
    - Support for anonymous binding is now enabled with LDAP server support.
- Multiple Domain Support for External Authentication - Multiple domains are supported as long as the all domains are searchable from the global catalog or available via referral.
- Config API availability - Configuration validation was added in 11.3 so validation could be done on configurations modified using the API. Prior validation was only done for entries added or edited in the UI, so some customers may currently have invalid configurations due to previous imports or migrations. Because of this, a re-import of an exported configuration may cause some validation errors. The first validation error seen will be shown in the UI on import - users can edit the exported file and import again. If an import fails without an error in the UI, please contact Customer Support
- Scalability to multiple TVCs with a single user interface. Please contact Customer Support before enabling this feature.

1.2 Components Affected

TruView Central (TVC), TruView Packet (TVP), TruView Flow (TVF)

1.3 Installation

Upgrade - Download the tar.gz to a local system, then login to the TruView UI, navigate to Administration/ADMIN/Software Update and BROWSE to load the file you downloaded.

Upgrade file location - my.netscout.com

Upgrade file - TruView-11.3.920-1.tar.gz

1.4 Known Issues

- **DE37005** - Security Warning Message when trying to setup the vTVF.ova
  - **Mitigation** - This only appears in the Vsphere 6.5 ESX; Message can be ignored
- **DE37003** - Sintrex - v11 - Packet Analysis -> Export to CSV not working on Mozilla Firefox.
  - **Mitigation**: Use Chrome or IExplorer
- **DE33682** - TruView supports creating up to 150 domains.
  - **Mitigation**: Additional domain adds will take significant time.
- **DE36987** - A rare race condition occurs in upgrade where Cassandra might not allow connections.
  - **Mitigation:** `sudo systemctl restart cassandra`
- **DE31544** - TVP 10G Snidely card Packet Filter leaking unwanted packets
  - **Mitigation:** Don't set 'Capture Only' filter
  - **Mitigation:** Set the Slicing size of 'Capture Only' filter(s) to 'Header Only' or 'Header +', and set all the 'Analysis + Capture' filter(s) to 'Full Packet'.

1.5 Defects Fixed

- **DE30607** - We now support replacing network devices. The old device must be deleted first before we send netflow from the new device. This only applies when the new device and the old device share the same IP address.
- **DE30664** – TVP Network Delay / EURT Alarms not completing v11.1
- **DE30852** - Alert link provides IP address instead of hostname
- **DE30900** - Dashboard page link sending to wrong site
- **DE31296** - OVA tv-configure.sh create ifcfg file, if one does not exist
- **DE31297** - New Devices on TVF not fully discovered
- **DE33284** - List of TVPs in Data Sources and Packet Filters are not kept in alignment
- **DE33306** - Support HTTPS-only for TVF Native GUI
- **DE33681** - ISO install supports R320 iDRAC as well as R320 DVD
- **DE33829** - Netflow device ip address changed and data for new device not showing in TVC
- **DE33861** - While editing Dashboards, the Interface Search within a graph is not working
- **DE33887** - Unable to rename servers
- **DE33949** - Customer can't copy User Group Templates to another User Group
- **DE33984** - Software update issue when loading wrong file
- **DE34253** - Alarms not able to set negative value to 0
- **DE35112** - Out of memory condition on small, legacy, distributed TVFs
- **DE34368** - Server Search is not returning all requested servers. Only returning one entry
- **DE35354** - several netflow devices using snmp v3 are not polling
- **DE35497** - Busiest Interfaces - Error 200 when using "Last 60 minutes"
- **DE35550** - Truview Central disable negative alert
- **DE35751** - TVP failing to publish
- **DE35781** - Unable to edit/delete some Custom Dashboards
- **DE35931** - Citrix is no longer part of "Application Type" under Custom Apps.

- **DE36097** - Propagating NetworkDevice and NetworkInterface changes to ElasticSearch
- **DE36612** - HTTP response header X-Frame-Options set to 'SAMEORIGIN' for portal and TVF native UI, which will guard against click-jacking by blocking our content from being hosted inside an iframe from another domain. This can be configured in /opt/tv/portal/server/config/env/all.js (tv-portal) or in /opt/tv/flow/fntracker_webapp/WEB-INF/web.xml (TVF).
- **DE36821** - SNMP polling from TVF causing device(s) CPU to spike

1.6 Security Fixes

- **(CVE-2018-1049)** - A race condition was found in systemd. This could result in automount requests not being serviced and processes using them could hang, causing denial of service.
- **(CVE-2017-7529)** - Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.
- **(CVE-2016-4450)** - os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.
- **(CVE-2018-2678)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.
- **(CVE-2018-2677)** - Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

- **(CVE-2018-2663)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.
- **(CVE-2018-2657)** - Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u171 and 7u161; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, JRockit. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.
- **(CVE-2018-2641)** - Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
- **(CVE-2018-2639)** - Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run

untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

- **(CVE-2018-2638)** - Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
- **(CVE-2018-2637)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.
- **(CVE-2018-2634)** - Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JGSS). Supported versions that are affected are Java SE: 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
- **(CVE-2018-2633)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple

protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.

- **(CVE-2018-2629)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JGSS). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.
- **(CVE-2018-2627)** - Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Installer). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to the Windows installer only.
- **(CVE-2018-2618)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.
- **(CVE-2018-2603)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE:

6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.

- **(CVE-2018-2602)** - Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: I18n). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded executes to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
- **(CVE-2018-2599)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.
- **(CVE-2018-2588)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: LDAP). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE

Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.

- **(CVE-2018-2582)** - Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 8u152 and 9.0.1; Java SE Embedded: 8u151. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.
- **(CVE-2018-2581)** - Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). Supported versions that are affected are Java SE: 7u161, 8u152 and 9.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
- **(CVE-2018-2579)** - Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.

- **(CVE-2017-1000257)** - A buffer overrun flaw was found in the IMAP handler of libcurl. By tricking an unsuspecting user into connecting to a malicious IMAP server, an attacker could exploit this flaw to potentially cause information disclosure or crash the application
- **(CVE-2017-13090)** - A stack-based and a heap-based buffer overflow flaws were found in wget when processing chunked encoded HTTP responses. By tricking an unsuspecting user into connecting to a malicious HTTP server, an attacker could exploit these flaws to potentially execute arbitrary code
- **(CVE-2017-13089)** - A stack-based and a heap-based buffer overflow flaws were found in wget when processing chunked encoded HTTP responses. By tricking an unsuspecting user into connecting to a malicious HTTP server, an attacker could exploit these flaws to potentially execute arbitrary code
- **(CVE-2017-3145)** - A use-after-free flaw leading to denial of service was found in the way BIND internally handled cleanup operations on upstream recursion fetch contexts. A remote attacker could potentially use this flaw to make named, acting as a DNSSEC validating resolver, exit unexpectedly with an assertion failure via a specially crafted DNS request.
- **(CVE-2017-3144)** - It was found that the DHCP daemon did not properly clean up closed OMAPI connections in certain cases. A remote attacker able to connect to the OMAPI port could use this flaw to exhaust file descriptors in the DHCP daemon, leading to a denial of service in the OMAPI functionality.