Haivision
NETWORK VIDEO

Scan Report: Retina - Kraken 2.0.1-6 (2015-05-15)

Report generated
Mon, 18 May 2015 17:20:02 -0500

Scan Summary

Report Filename
Retina-Kraken-2.0.1-6-20150515.xml

Description
Scheduled scan

Date of Scan
2015-05-15 15:10:41

Scanner version
5.19.11

Scanner audits revision
2906

Scanner audit groups
All Audits, All STIG Audits, IAVA, IAVA Alerts, IAVA-ACERT, IAVA-AFCERT, IAVA-NAVCIRT, SANS20 (Unix)

Target Summary

Product / Version / Build
Kraken 2.0.1-6

Host OS
CentOS release 6.6 (Final)

Priority Summary(Cat I and II findings):

For detailed information, see the Detailed Findings section below.

Audit ID	Audit Name	Sev Code	Risk	Categorization
46310	CESA-2015:0864 - kernel security update	Category I	High	Ack (Fixed in future update)
46289	Magento Ecommerce Platform Remote Code Execution Vulnerability	Category I	High	False Pos (rejected)
34966	Stunnel Multiple Vulnerabilities (20140814) - UNIX/Linux	Category I	High	False Pos (fix installed)
34419	Stunnel Multiple Vulnerabilities (20140618) - UNIX/Linux	Category I	High	False Pos (fix installed)
18467	Stunnel Buffer Overflow (20130303) - UNIX/Linux	Category I	High	False Pos (fix installed)
19272	PHP Buffer Overflow Vulnerability (20130606)	Category I	Medium	False Pos (rejected)
46281	CESA-2015:0863 - glibc security update	Category II	Medium	Ack (Fixed in future update)
33246	SSL/TLS RC4 Cipher Suites Supported	Category II	Medium	Ack (No fix, unmitigable)

46008	CESA-2015:0794 - krb5 security update	Category II	Medium	Ack (Fixed in future update)
35464	Stunnel OpenSSL Multiple Vulnerabilities (POODLE) < 5.06 - Linux/UNIX	Category II	Medium	False Pos (fix installed)
11892	SSL Weak Cipher Supported	Category II	Medium	False Pos (fix installed)

Detailed Findings:

Audit ID	Audit Name	Sev Code	Risk	Categorization
46310	CESA-2015:0864 - kernel security update	Category I	High	Ack (Fixed in future update)

Audit Description

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security has rated this update as having Important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

* A flaw was found in the way seunshare, a utility for running executables under a different security context, used the capng_lock functionality of the libcap-ng library. The subsequent invocation of suid root binaries that relied on the fact that the setuid() system call, among others, also sets the saved set-user-ID when dropping the binaries' process privileges, could allow a local, unprivileged user to potentially escalate their privileges on the system. Note: the fix for this issue is the kernel part of the overall fix, and introduces the PR_SET_NO_NEW_PRIVS functionality and the related SELinux exec transitions support. (CVE-2014-3215, Important)

* A use-after-free flaw was found in the way the Linux kernel's SCTP implementation handled authentication key reference counting during INIT collisions. A remote attacker could use this flaw to crash the system or, potentially, escalate their privileges on the system. (CVE-2015-1421, Important)

* It was found that the Linux kernel's KVM implementation did not ensure that the host CR4 control register value remained unchanged across VM entries on the same virtual CPU. A local, unprivileged user could use this flaw to cause a denial of service on the system. (CVE-2014-3690, Moderate)

* An out-of-bounds memory access flaw was found in the syscall tracing functionality of the Linux kernel's perf subsystem. A local, unprivileged user could use this flaw to crash the system. (CVE-2014-7825, Moderate)

* An out-of-bounds memory access flaw was found in the syscall tracing functionality of the Linux kernel's ftrace subsystem. On a system with ftrace syscall tracing enabled, a local, unprivileged user could use this flaw to crash the system, or escalate their privileges. (CVE-2014-7826, Moderate)

* It was found that the Linux kernel memory resource controller's (memcg) handling of OOM (out of memory) conditions could lead to deadlocks. An attacker able to continuously spawn new processes within a single memory-constrained cgroup during an OOM event

could use this flaw to lock up the system. (CVE-2014-8171, Moderate)

* A race condition flaw was found in the way the Linux kernel keys management subsystem performed key garbage collection. A local attacker could attempt accessing a key while it was being garbage collected, which would cause the system to crash. (CVE-2014-9529, Moderate)

* A stack-based buffer overflow flaw was found in the TechnoTrend/Hauppauge DEC USB device driver. A local user with write access to the corresponding device could use this flaw to crash the kernel or, potentially, elevate their privileges on the system. (CVE-2014-8884, Low)

* An information leak flaw was found in the way the Linux kernel's ISO9660 file system implementation accessed data on an ISO9660 image with RockRidge Extension Reference (ER) records. An attacker with physical access to the system could use this flaw to disclose up to 255 bytes of kernel memory. (CVE-2014-9584, Low)

Red Hat would like to thank Andy Lutomirski for reporting CVE-2014-3215 and CVE-2014-3690, Robert Swiecki for reporting CVE-2014-7825 and CVE-2014-7826, and Carl Henrik Lunde for reporting CVE-2014-9584. The CVE-2015-1421 issue was discovered by Sun Baoliang of Red Hat.

This update also fixes several bugs. Documentation for these changes is available from the Technical Notes document linked to in the References section.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

Related codes CVE-2015-1421, CVE-2014-8884, CVE-2014-3215, CVE-2014-7826, CVE-2014-8171, CVE-2014-9584, CVE-2014-7825, CVE-2014-9529, CVE-2014-3690

Haivision response

Categorization
Ack (Fixed in future update)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3284

Details
Fix in RHSA-2015:0864-1 Tracked in ticket KRAK-1034

Minimum Update Req.
kernel-2.6.32-504.16.2.el6.src.rpm

Audit ID	Audit Name	Sev Code	Risk	Categorization
46289	Magento Ecommerce Platform Remote Code Execution Vulnerability	Category I	High	False Pos (rejected)

Audit Description eBay's eCommerce platform Magento is prone to a remote code execution vulnerability. If successfully exploited, an attacker can gain customers' credit card information.

Haivision response

Categorization

Build/install verified

False Pos (rejected)

Kraken 2.0.1-6()

Verified as of (date)

May 8 2015

Response ID reference

3267

Details

Audit ID	Audit Name	Sev Code	Risk	Categorization
34966	Stunnel Multiple Vulnerabilities (20140814) - UNIX/Linux	Category I	High	False Pos (fix installed)

Audit Description Stunnel contains multiple vulnerabilities due to the errors found in OpenSSL.

Related codes CVE-2014-3508, CVE-2014-3505, CVE-2014-3512, CVE-2014-3509, CVE-2014-3511, CVE-2014-3507, CVE-2014-5139, CVE-2014-3506, CVE-2014-3510

Haivision response

Categorization

False Pos (fix installed)

Build/install verified

Kraken 2.0.1-6()

Verified as of (date)

May 8 2015

Response ID reference

3261

Details

Fixed in the installed version of the affected package.

Minimum Update Req.

openssl-1.0.1e-30.el6_6.4.i686 openssl-1.0.1e-30.el6_6.4.x86_64

Audit ID	Audit Name	Sev Code	Risk	Categorization
34419	Stunnel Multiple Vulnerabilities (20140618) - UNIX/Linux	Category I	High	False Pos (fix installed)

Audit Description Stunnel contains multiple vulnerabilities which can lead to sensitive information disclosure, denial of service, and arbitrary code execution, by sending malicious requests to the affected system.

Related codes CVE-2014-0198, CVE-2014-0224, CVE-2014-0221, CVE-2014-3470, CVE-2010-5298, CVE-2014-0195

Haivision response

Categorization

False Pos (fix installed)

Build/install verified

Kraken 2.0.1-6()

Verified as of (date)

May 8 2015

Response ID reference

3263

Details

Fixed in the installed version of the affected package.

Audit ID	Audit Name	Sev Code	Risk	Categorization
18467	Stunnel Buffer Overflow (20130303) - UNIX/Linux	Category I	High	False Pos (fix installed)

Audit Description Stunnel contains a vulnerability due to incorrect integer conversion when handling a crafted request which may trigger a buffer overflow. Successful exploitation may result in arbitrary code execution.

Related codes CVE-2013-1762

Haivision response

Categorization
False Pos (fix installed)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3262

Details
Red Hat backported the fix into stunnel-4.29-3.el6_4.i686.rpm, which is currently installed on Kraken.

Minimum Update Req.
stunnel-4.29-3.el6_4.i686.rpm

Audit ID	Audit Name	Sev Code	Risk	Categorization
19272	PHP Buffer Overflow Vulnerability (20130606)	Category I	Medium	False Pos (rejected)

Audit Description PHP before 5.4.16 and 5.3.26 contains a heap-based buffer overflow in the "php_quot_print_encode()" function when parsing passed strings. Successful exploitation may result in execution of arbitrary code or a denial of service condition.

Related codes CVE-2013-2110

Haivision response

Categorization
False Pos (rejected)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3281

Details
Not Vulnerable. This issue does not affect the version of php as shipped with Red Hat Enterprise Linux 5 and 6. This issue does not affect the version of php53 as shipped with Red Hat Enterprise Linux 5.

Audit ID	Audit Name	Sev Code	Risk	Categorization
46281	CESA-2015:0863 - glibc security update	Category II	Medium	Ack (Fixed in future update)

Updated glibc packages that fix two security issues and one bug are now available for Red

Audit Description

Hat Enterprise Linux 6.

Red Hat Product Security has rated this update as having Moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the Name Server Caching Daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

A buffer overflow flaw was found in the way glibc's gethostbyname_r() and other related functions computed the size of a buffer when passed a misaligned buffer as input. An attacker able to make an application call any of these functions with a misaligned buffer could use this flaw to crash the application or, potentially, execute arbitrary code with the permissions of the user running the application. (CVE-2015-1781)

It was discovered that, under certain circumstances, glibc's getaddrinfo() function would send DNS queries to random file descriptors. An attacker could potentially use this flaw to send DNS queries to unintended recipients, resulting in information disclosure or data loss due to the application encountering corrupted data. (CVE-2013-7423)

The CVE-2015-1781 issue was discovered by Arjun Shankar of Red Hat.

This update also fixes the following bug:

* Previously, the nscd daemon did not properly reload modified data when the user edited monitored nscd configuration files. As a consequence, nscd returned stale data to system processes. This update adds a system of inotify-based monitoring and stat-based backup monitoring for nscd configuration files. As a result, nscd now detects changes to its configuration files and reloads the data properly, which prevents it from returning stale data. (BZ#1194149)

All glibc users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

Related codes CVE-2015-1781, CVE-2013-7423

Haivision response

Categorization
Ack (Fixed in future update)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3285

Details
Fixed in a future update. Fix in RHSA-2015:0863-1 Tracked in ticket KRAK-1035

Minimum Update Req.
glibc-2.12-1.149.el6_6.7.src.rpm

Audit ID	Audit Name	Sev Code	Risk	Categorization
33246	SSL/TLS RC4 Cipher Suites Supported	Category II	Medium	Ack (No fix, unmitigable)

Audit Description

The remote host allows the use of RC4 cipher suites. The RC4 cipher generation of a pseudo-random stream of bytes is flawed to allow small biases into the stream, decreasing its randomness. If plaintext is encrypted over and over and an attacker is able to obtain millions of ciphertexts, the attacker may be able to retrieve the plaintext from the stream.

Related codes

CVE-2013-2566

Haivision response

Categorization
Ack (No fix, unmitigable)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3279

Details
Will not be fix in CENTOS 6. https://access.redhat.com/security/cve/CVE-2013-2566

Audit ID	Audit Name	Sev Code	Risk	Categorization
46008	CESA-2015:0794 - krb5 security update	Category II	Medium	Ack (Fixed in future update)

Audit Description

Updated krb5 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security has rated this update as having Moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Kerberos is a networked authentication system which allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos KDC.

The following security issues are fixed with this release:

A use-after-free flaw was found in the way the MIT Kerberos libgssapi_krb5 library processed valid context deletion tokens. An attacker able to make an application using the GSS-API library (libgssapi) could call the gss_process_context_token() function and use this flaw to crash that application. (CVE-2014-5352)

If kadmind were used with an LDAP back end for the KDC database, a remote, authenticated attacker who has the permissions to set the password policy could crash kadmind by attempting to use a named ticket policy object as a password policy for a principal. (CVE-2014-5353)

It was found that the krb5_read_message() function of MIT Kerberos did not correctly sanitize input, and could create invalid krb5_data objects. A remote, unauthenticated attacker could use this flaw to crash a Kerberos child process via a specially crafted request. (CVE-2014-5355)

A double-free flaw was found in the way MIT Kerberos handled invalid External Data Representation (XDR) data. An authenticated user could use this flaw to crash the MIT Kerberos administration server (kadmind), or other applications using Kerberos libraries, via specially crafted XDR packets. (CVE-2014-9421)

It was found that the MIT Kerberos administration server (kadmind) incorrectly accepted certain authentication requests for two-component server principal names. A remote attacker able to acquire a key with a particularly named principal (such as "kad/x") could use this flaw to impersonate any user to kadmind, and perform administrative actions as that user. (CVE-2014-9422)

Red Hat would like to thank the MIT Kerberos project for reporting CVE-2014-5352, CVE-2014-9421, and CVE-2014-9422. The MIT Kerberos project acknowledges Nico Williams for assisting with the analysis of CVE-2014-5352.

All krb5 users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

Related codes CVE-2014-9422, CVE-2014-5352, CVE-2014-9421, CVE-2014-5355, CVE-2014-5353

Haivision response

Categorization
Ack (Fixed in future update)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3283

Details
Issue tracked in KRAK-1028 Fixed in RHSA-2015:0794-1

Minimum Update Req.
krb5-libs-1.10.3-37.el6_6.i686.rpm

Audit ID	Audit Name	Sev Code	Risk	Categorization
35464	Stunnel OpenSSL Multiple Vulnerabilities (POODLE) < 5.06 - Linux/UNIX	Category II	Medium	False Pos (fix installed)

Audit Description Multiple vulnerabilities found in Stunnel versions prior to 5.06 that can lead to a denial of service and an attacker taking advantage of the 'POODLE' issue.

Related codes CVE-2014-3568, CVE-2014-3513, CVE-2014-3567, CVE-2014-3566

Haivision response

Categorization
False Pos (fix installed)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3282

Details
Current build contains the fix for OpenSSL. (RHSA-2014:1652) Redhat reports CVE-2014-3568 as Not Vulnerable

Minimum Update Req.
openssl-1.0.1e-30.el6_6.2.i686.rpm

Audit ID	Audit Name	Sev Code	Risk	Categorization
11892	SSL Weak Cipher Supported	Category II	Medium	False Pos (fix installed)

Audit Description Retina has detected that the targeted SSL service supports cryptographically weak encryption ciphers An attacker may be able to leverage weaknesses in the encryption ciphers to gain access to sensitive information.

Related codes CVE-2013-2566

Haivision response

Categorization
False Pos (fix installed)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3280

Details
Kraken properly rejects SSLv2

Audit ID	Audit Name	Sev Code	Risk	Categorization
34304	libtasn1 3.5 and Prior Multiple Vulnerabilities	Category III	Low	False Pos (fix installed)

Audit Description libtasn1 contains multiple unknown vulnerabilities which may be exploited to have an unknown impact.

Related codes CVE-2014-3468, CVE-2014-3467, CVE-2014-3469

Haivision response

Categorization
False Pos (fix installed)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3277

Details

Minimum Update Req.
libtasn1-2.3-6.el6_5.x86_64

Audit ID	Audit Name	Sev Code	Risk	Categorization
32626	libcURL Security Bypass (20140131)	Category III	Low	False Pos (fix installed)

Audit Description libcURL prior to 7.35.0 contains an error when re-using recent authenticated connections when processing new NTLM-authenticated requests. Successful exploitation may allow an attacker to perform certain operations with the credentials of a recent NTLM authenticated user.

Related codes CVE-2014-0015

Haivision response

Categorization
False Pos (fix installed)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3278

Details
Fixed in installed version of the affected packages (RHSA-2014:0561).

Minimum Update Req.
curl-7.19.7-37.el6_5.3.x86_64.rpm libcurl-7.19.7-37.el6_5.3.x86_64.rpm

Audit ID	Audit Name	Sev Code	Risk	Categorization
12374	SSL Certificate Self-Signed	Category III	Low	Ack (No fix, supported mitigable)

Audit Description Retina has detected that the certificate on target is self-signed. Self-signed certificates can provide underlying cryptographic functionality, but cannot guarantee the origin of the certificate is trusted.

Haivision response

Categorization
Ack (No fix, supported mitigable)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3276

Details
Trusted certs can be purchased by customer. Tech support can assist with installation.

Audit ID	Audit Name	Sev Code	Risk	Categorization
3688	ICMP Timestamp Request	Category III	Low	Ack (No fix, unsupported mitigable)

Audit Description ICMP Timestamp request is allowed from arbitrary hosts.

Related codes CVE-1999-0524

Haivision response

Categorization
Ack (No fix, unsupported mitigable)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3275

Details
Firewall configuration required. Firewalls are not configured and not supported on Kraken appliances.

Audit ID	Audit Name	Sev Code	Risk	Categorization
45860	SSL/TLS Cipher Block Chaining Cipher Suites Supported	Category IV	Information	No Impact

Audit Description

The remote host supports Cipher Block Chaining (CBC) mode SSL/TLS ciphers. These ciphers are more secure than Electronic Codebook (ECB) mode ciphers but can lead to information disclosure if used improperly.

Haivision response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3274

Details
Informational audit; no response required.

Audit ID	Audit Name	Sev Code	Risk	Categorization
45856	SSL/TLS Cipher Suites Supported	Category IV	Information	No Impact

Audit Description

The remote host was found to support the following set of SSL/TLS ciphers for encrypting communications.

Haivision response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3273

Details
Informational audit; no response required.

Audit ID	Audit Name	Sev Code	Risk	Categorization
44296	HTTP Zero Content-Length Detected	Category IV	Information	No Impact

Audit Description

Retina has detected that the remote site responded with a content length of zero.

Haivision response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3272

Details
Informational check. No response needed.

Audit ID	Audit Name	Sev Code	Risk	Categorization
14328	HTTP Server Cookies Detected	Category IV	Information	No Impact

Audit Description

Retina has detected that the target web server uses cookies to track HTTP sessions. Although HTTP is a stateless protocol, servers may use mechanisms as a generic form of managing login sessions.

Haivision response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3271

Details
Kraken systems utilize cookies via HTTPS to store session identifiers.

Audit ID	Audit Name	Sev Code	Risk	Categorization
18525	SSH Server Detected	Category IV	Information	Ack (No fix, unsupported mitigable)

Audit Description

Retina has detected an instance of an SSH server.

Haivision response

Categorization
Ack (No fix, unsupported mitigable)

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3270

Details
Kraken systems utilize SSH to provide remote access to the administration console.

Audit ID	Audit Name	Sev Code	Risk	Categorization
12349	GRE Protocol Support Detected	Category IV	Information	No Impact

Audit Description

Retina has detected that the targeted system supports protocol 47, Generic Route Encapsulation (GRE). This protocol provides the ability to encapsulate packets within an IP tunnel to create a virtual point-to-point link (i.e. PPTP) between systems. GRE is inherently insecure due to the lack of built-in encryption and incidentally may be improperly configured. An attacker may potentially leverage weaknesses in the protocol or resulting configuration to intercept traffic or gain unauthorized access to systems.

Haivision response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3269

Details
Informational audit; no response required.

Audit ID	Audit Name	Sev Code	Risk	Categorization
12355	SSL Certificate Public Key Algorithm	Category IV	Information	No Impact

Audit Description

This is an informational check. Retina has detected the certificate's public key algorithm.

Haivision response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3268

Details
Informational audit; no response required.

Audit ID	Audit Name	Sev Code	Risk	Categorization
12610	SSL Certificate Version	Category IV	Information	No Impact

Audit Description

This is an informational check. Retina has detected the certificate's version.

Haivision response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3266

Details
Informational audit; no response required.

Audit ID	Audit Name	Sev Code	Risk	Categorization
12611	IPv6 Protocol Support Detected	Category IV	Information	No Impact

Audit Description

Retina has detected that the targeted system supports an IPv6 protocol. These protocols include: HOPOPT (protocol 0), IPv6 encapsulation (protocol 41), IPv6-Route (protocol 43), IPv6-Frag (protocol 44), IPv6-ICMP (protocol 58), IPv6-NoNxt (protocol 59), and IPv6-Opts (protocol 60).

Haivision

response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3265

Details
Informational audit; no response required.

Audit ID	Audit Name	Sev Code	Risk	Categorization
7301	HTTP 1.1 Protocol Detected	Category IV	Information	No Impact

Audit Description

This is an informational check. Retina has detected version 1.1 of the HTTP Protocol on the target system.

Haivision response

Categorization
No Impact

Build/install verified
Kraken 2.0.1-6()

Verified as of (date)
May 8 2015

Response ID reference
3264

Details
Informational check. No response needed.

Category Explanation:

Category	Description
False Pos (Total)	False Positive, no basis for finding demonstrated.
No Impact	Informational checks and other innocuous findings which have no security implication, and are not a false positive.
False Pos (fix installed)	False Positive, Legitimate finding has been fixed in the indicated release, but scanner has reported the finding. Typically related to vendor-backported system packaged
False Pos (affected components not installed)	False Positive, Finding indicates software packages that are demonstrated not to be installed on the system.
False Pos (rejected)	False Positive, Finding has been rejected based on criteria for impact and reasonable operating environments. Typically this designation is given by the OS vendor.
Ack (Fixed in current update)	Acknowledged, has been demonstrated fixed in currently available updates to the product.
Ack (Mitigation configured)	Acknowledged. As configured, behavior is mitigated.
Ack (Fixed in future update)	Acknowledged, is expected to be fixed in upcoming updates to the product
	Acknowledged, no supported fix is expected to be released in upcoming updates to the product. Supported mitigation

Ack (No fix, supported mitigable)	steps are available which may mitigate the issue which have been certified supportable in the product.
Ack (No fix, unsupported mitigable)	Acknowledged, no supported fix is expected to be released in upcoming updates to the product. Unsupported mitigation steps are available which may mitigate the issue while voiding support in this configuration
Unknown	Finding has not been researched for impact, and should be considered an open finding.
Ack (No fix, unmitigable)	Acknowledged, no supported fix is expected to be released in upcoming updates to the product. There is no reasonable mitigation step and the issue is considered an open finding.

The authors of this document have made a good-faith effort to ensure that the information reported is truthful and accurate, but any information contained is subject to future review and revision. Any views or opinions presented in this document are solely those of the author(s) and do not necessarily represent those of the company. Haivision Network Video accepts no liability for the content of this document, or for the results of any actions taken on the basis of the information provided, unless that information is subsequently confirmed in writing.

This document and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. This document contains confidential information. If you are not the named addressee you should not disseminate, distribute or copy this document.