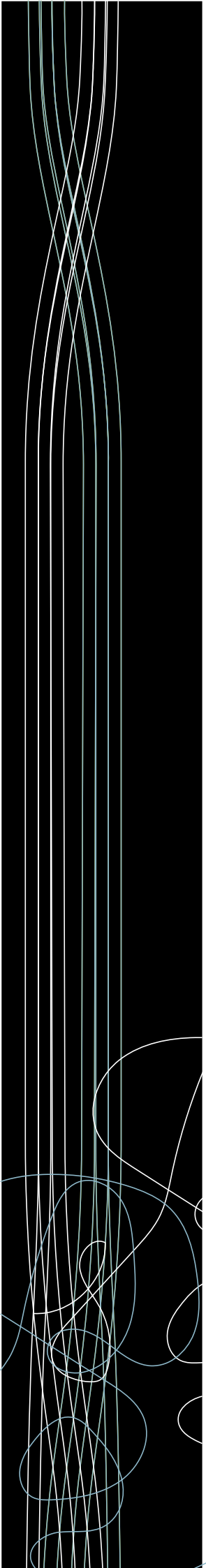


SECURITY BULLETIN

OpenSSL Vulnerability

November 09, 2022

The OpenSSL Project recently announced CRITICAL vulnerabilities associated with OpenSSL versions 3.0 and higher that include:

- CVE-2022-3602 is an arbitrary 4-byte stack buffer overflow that could trigger crashes or lead to remote code execution (RCE).
- CVE-2022-3786 can be exploited by attackers via malicious email addresses to trigger a denial-of-service state via a buffer overflow.

These vulnerabilities were later downgraded from CRITICAL to HIGH (CVSS score 8.8 from 9.0). OpenSSL version 3.0.7, released on November 1, 2022, addresses these vulnerabilities. The following document provides important information to understand and protect your assets from these vulnerabilities.

What is OpenSSL?

OpenSSL is a widely used open-source cryptography utility implemented to secure web traffic exchanged between a client and server. It is used to generate public and private keys, install SSL/TLS certificates, verify certificate information, and provide encryption.

Most web servers across the Internet and within intranets use SSL certificates to secure connections and the website being browsed. These certificates are traditionally generated by OpenSSL.

How concerned should you be about this vulnerability?

OpenSSL can be misused if the vulnerable version is in use. The good news is that this vulnerability impacts a very specific version of OpenSSL and patching quickly will address any associated risks.

A flaw in OpenSSL has previously affected businesses. In April 2014, OpenSSL's Heartbleed flaw was discovered. Numerous web servers, including those running popular websites like Yahoo, included it. Security teams rushed to apply updates because the vulnerability was simple to exploit.

How is the vulnerability exploited?

Both CVE-2022-3602 and CVE-2022-3786 vulnerabilities are prone to buffer overflow attacks that can perform Remote Code Execution (RCE) or expose contents of the memory that contains private keys or proprietary information.

The chances of these vulnerabilities getting abused are low because one of the conditions is a malformed certificate signed by a trusted CA.

The issue lies in the verification process of certificates that OpenSSL performs for certificate-based authentication. The exploitation of the vulnerabilities could allow an attacker to launch a Denial of Service (DoS) or even an RCE attack.

Patches for the two weaknesses found in OpenSSL v3.0.0 to v3.06 have now been released.

Which OpenSSL versions are vulnerable?

- OpenSSL versions 3.0 and above are vulnerable.
- OpenSSL 3.0.0, the first stable version of OpenSSL 3.0, was released in September 2021, about one year ago. Any older operating systems prior to 3.0.0 are not impacted by this vulnerability.
- Open SSL version 3.0.0 to 3.0.6 are affected by this vulnerability.
- OpenSSL version 3.0.7 includes the fix for the critical vulnerability.

CRITICAL Severity: This affects common configurations, which are also likely to be exploitable. Among these are significant disclosures of server memory (potentially revealing user information), vulnerabilities that are easily exploitable to compromise server private keys remotely, or situations where remote code execution is possible. We will keep these issues private and release a new version of all supported versions as soon as possible.

HIGH Severity: This includes issues that are of a lower risk than CRITICAL, perhaps due to affecting fewer common configurations or which are less likely to be exploitable. These issues will be kept private and will trigger a new release of all supported versions. We will attempt to keep the time these issues are private to a minimum; our aim would be no longer than a month, where this is something under our control.

What should security teams do?

Use Ordr's vulnerability scanner or any other scanner with similar capabilities to identify if your organization uses the vulnerable OpenSSL version. If you are using OpenSSL 3.0, patch immediately.

Is the Ordr platform impacted by the OpenSSL vulnerability?

Ordr has reviewed our usage of OpenSSL. This vulnerability does not impact Ordr as we do not use the impacted version.

How Ordr helps

Ordr Scanner

Ordr uses an unauthenticated way to get information about Open SSL versions while other scanners rely on an authenticated approach that requires full credentials. The Ordr scanner also uses tools like Nmap to find open ports as a precursor before determining the OpenSSL version. The Ordr Scanner uses the following:

- HTTPS headers, SSH headers, and credentialed scans to get the information.
- For assets that do have an open HTTP port, a cURL command can be used to determine the SSL version.
- For assets that do not have an open HTTP port, an SSH command can be used to determine the SSL version.

Sample Ordr Scanner SSL command

```
curl -s -I abcd.com
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=iso-8859-1
Content-Length: 229
Connection: keep-alive
Date: Fri, 04 Nov 2022 05:26:33 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16 OpenSSL/1.0.2k-fips
Location: https://www.abcd.com/
Via: 1.1 varnish (Varnish/6.0), 1.1 22dc875d744f932282ce89367c98a9de.cloudfront.net(CloudFront)
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
X-Amz-Cf-Pop: SFO53-C1
X-Amz-Cf-Id: IQtd4xNPyLgvKHBfB39noPFh7hXdfTic_SYKQDWeCGQHNw2HdjIyLQ==
Age: 537
```

Sample Ordr Scanner SSH command

```
cpnadmin@ubuntu22-server:~$ ssh -v 10.30.11.184
OpenSSH_8.9p1 Ubuntu-3, OpenSSL 3.0.2 15 Mar 2022
debug1: Reading configuration data /etc/ssh/ssh_config
```

Detecting Exploit Attempts with a Signature Based IDS

Once the Ordr Scanner has detected all assets impacted by the vulnerability, the next step is to determine if the vulnerability is being exploited. Ordr has a signature-based intrusion detection engine that can scan for this and other exploits. Ordr has pushed the latest signature to all customers to identify and alert if malicious activity involving OpenSSL is detected.

Example signature to identify a potential exploit

```
alert tcp any any -> any any (msg:"SERVER-OTHER OpenSSL x509 crafted email address buffer overflow
attempt"; flow:established; content:"|06 03 55 1D 1E 01 01|"; content:"|04 82|"; within:2; distance:1;
content:"|30 82|"; within:2; distance:2; content:"|82|"; within:1; distance:3; content:"|30 82|";
within:2; distance:2; content:"|81 82|"; within:2; distance:2; byte_test:2,>,500,0,relative;
content:"xn--"; within:4; distance:2; fast_pattern; metadata:policy balanced-ips drop, policy
connectivity-ips drop, policy max-detect-ips drop, policy security-ips drop, ruleset community,
service ssl; reference:cve,2022-3602; classtype:attempted-user; sid:60790; rev:1;)
```

- CVS-2022-3602 - Detection of this pattern was done using IDS Signatures.
- A buffer overflow can be triggered by sending an X.509 certificate with a specially crafted email address in the “id-on-SmtpUTF8Mailbox” field (OID 1.3.6.1.5.5.7.8.9), resulting in a crash (Denial of Service - DoS) or potentially remote code execution on a vulnerable client or server. Potential opportunities for exploitation can occur if a server requests authentication information after a malicious client connects or if a client connects to a malicious server, which would then make the client vulnerable.
- “OpenSSL x509 crafted email address buffer overflow attempt” is detected with the following signature.

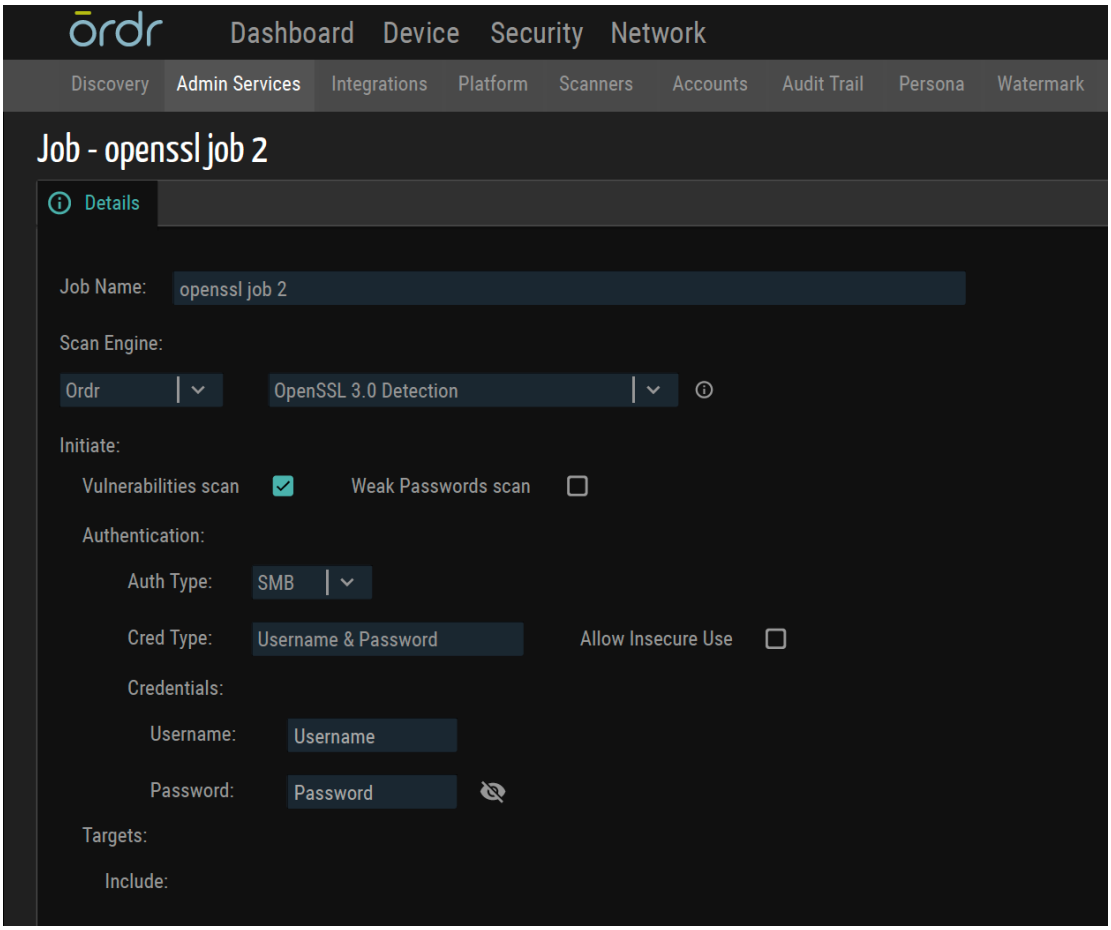


Figure 1: Ordr OpenSSL scan launch screen

Openssl3.0_detect_1667927687_1556_scan

IP	MAC	OpenSSL 3.0	SCANNED TIME	
10.30.11.146	00:0C:29:01:81:97	No	11/08/2022 5:15:19 PM	
10.30.11.195	00:0C:29:14:02:05	Yes	11/08/2022 5:15:19 PM	
10.30.11.184	00:0C:29:7C:EB:10	No	11/08/2022 5:15:19 PM	

Figure 2: OpenSSL jobs status with reports

Scanning Job List

Total 11 Scanning Jobs

Search currently visible fields ... Filter Saved Queries

No.	Job Name	Scan Type	Scan Engine	Last Run Status
1	tenablescan6355	Vulnerabilities	Tenable	Completed at 1/19/1970, 4:47:00 PM
2	ScanJob	Vulnerabilities	Ordr	Completed at 10/28/2022, 10:29:47 AM
3	openVasScan4307	Vulnerabilities	Ordr	Completed at 10/29/2022, 12:20:00 AM
4	Openssl3.0_detect	Vulnerabilities	Ordr	Completed at 11/8/2022, 9:15:19 AM
5	pscan25304	Weak Passwords	Ordr	Completed at 2/10/2022, 12:13:48 AM
6	pscan1800	Weak Passwords	Ordr	Completed at 2/10/2022, 12:47:26 AM
7	pscan4980	Weak Passwords	Ordr	Completed at 2/10/2022, 12:54:32 AM
8	Log4jUnsaved Job	Vulnerabilities	Ordr	Completed at 2/11/2022, 4:40:05 PM
9	openVasScan4307	Weak Passwords	Ordr	Completed at 2/9/2022, 11:30:22 PM
10	rapidscan6624	Vulnerabilities	Rapid7	Completed at 2/9/2022, 6:45:15 AM
11	Log4jUnsaved1	Vulnerabilities	Ordr	Error: Devices not scanned for unspecified reasons=["10.80.24.84"]

Figure 3: Scanning job list

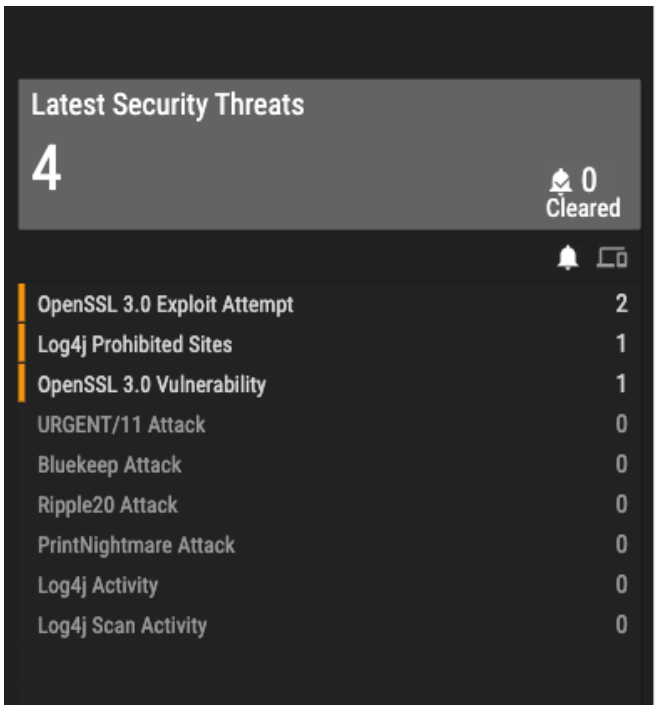


Figure 4: Latest security threat

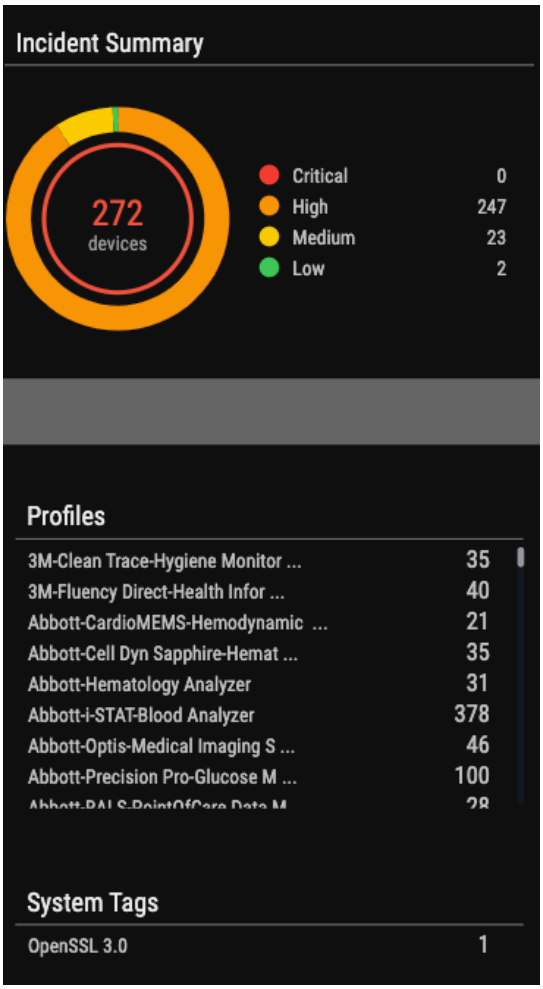
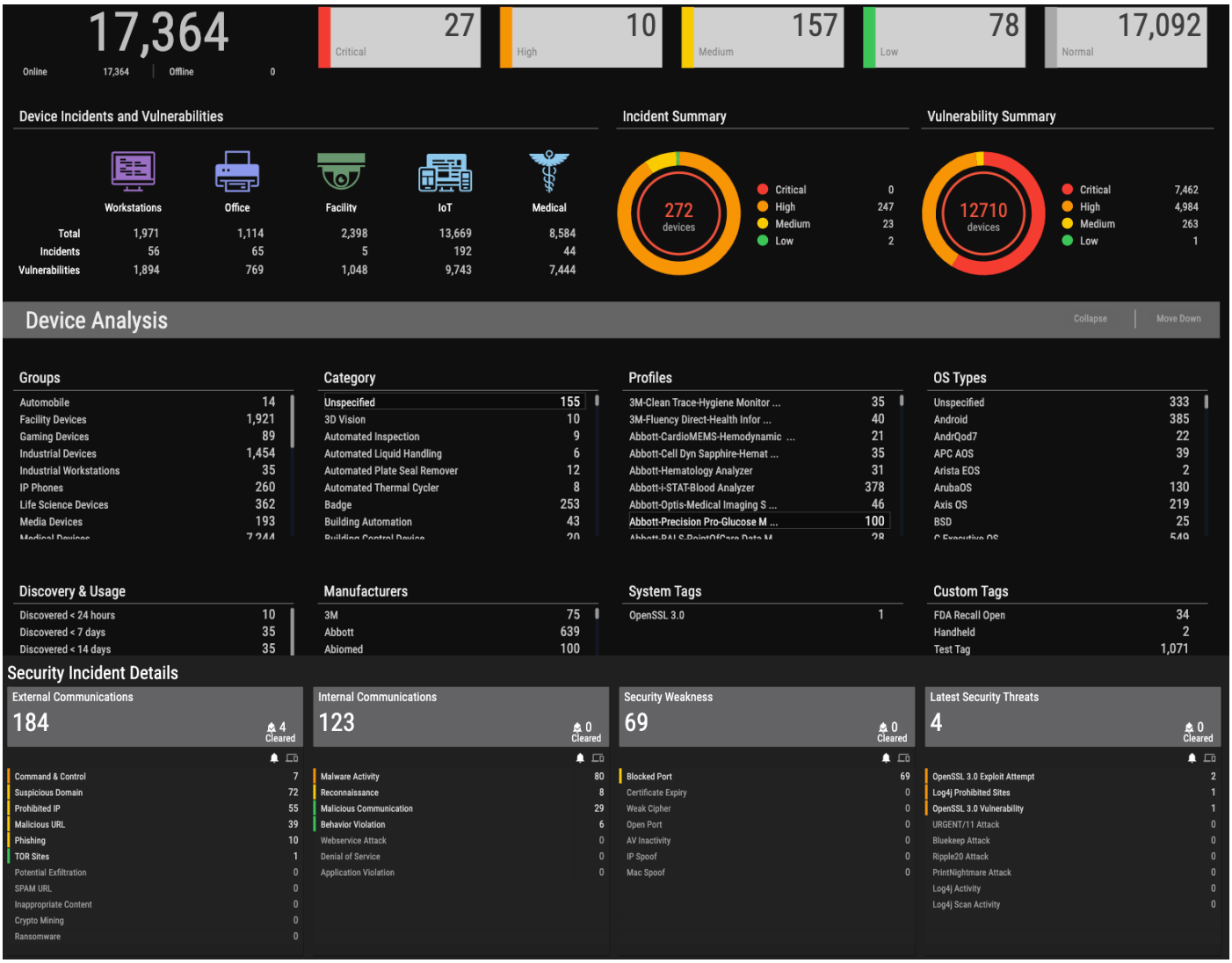
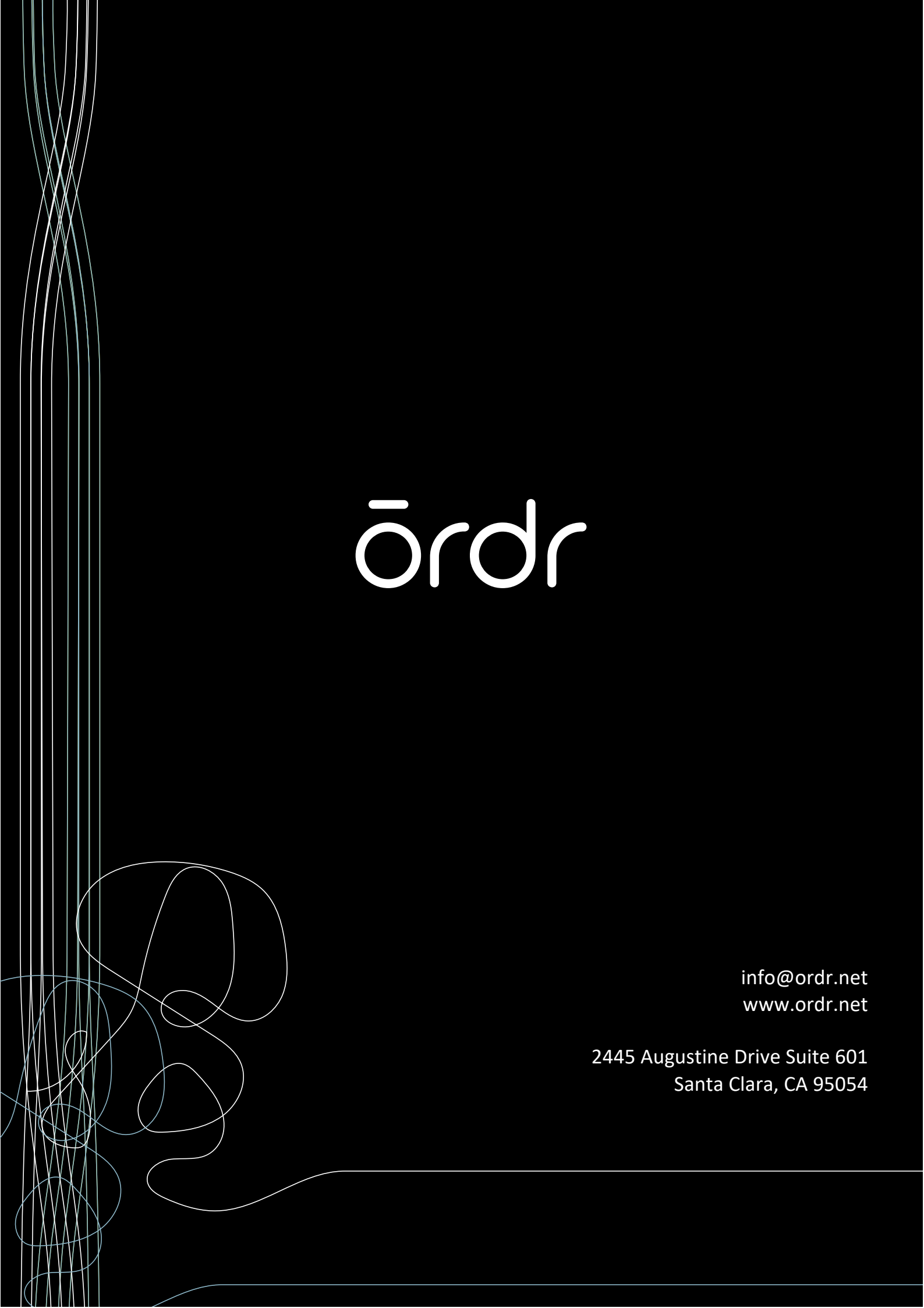


Figure 5: Incident Summary


17,364
Online 17,364 Offline 0
27 Critical
10 High
157 Medium
78 Low
17,092 Normal
Device Incidents and Vulnerabilities
Workstations Office Facility IoT Medical
Total 1,971 1,114 2,398 13,669 8,584
Incidents 56 65 5 192 44
Vulnerabilities 1,894 769 1,048 9,743 7,444
Incident Summary
272 devices
Critical 0
High 247
Medium 23
Low 2
Vulnerability Summary
12710 devices
Critical 7,462
High 4,984
Medium 263
Low 1
Device Analysis
Collapse
Move Down
Groups
Automobile 14
Facility Devices 1,921
Gaming Devices 89
Industrial Devices 1,454
Industrial Workstations 35
IP Phones 260
Life Science Devices 362
Media Devices 193
Category
Unspecified 155
3D Vision 10
Automated Inspection 9
Automated Liquid Handling 6
Automated Plate Seal Remover 12
Automated Thermal Cycler 8
Badge 253
Building Automation 43
Profiles
3M-Clean Trace-Hygiene Monitor ... 35
3M-Fluency Direct-Health Infor ... 40
Abbott-CardioMEMS-Hemodynamic ... 21
Abbott-Cell Dyn Sapphire-Hemat ... 35
Abbott-Hematology Analyzer 31
Abbott-i-STAT-Blood Analyzer 378
Abbott-Optis-Medical Imaging S ... 46
Abbott-Precision Pro-Glucose M ... 100
OS Types
Unspecified 333
Android 385
AndrQod7 22
APC AOS 39
Arista EOS 2
ArubaOS 130
Axis OS 219
BSD 25
Discovery & Usage
Discovered < 24 hours 10
Discovered < 7 days 35
Discovered < 14 days 35
Manufacturers
3M 75
Abbott 639
Abiomed 100
System Tags
OpenSSL 3.0 1
Custom Tags
FDA Recall Open 34
Handheld 2
Test Tag 1,071
Security Incident Details
External Communications
184
4 Cleared
Command & Control 7
Suspicious Domain 72
Prohibited IP 55
Malicious URL 39
Phishing 10
TOR Sites 1
Potential Exfiltration 0
SPAM URL 0
Inappropriate Content 0
Crypto Mining 0
Ransomware 0
Internal Communications
123
0 Cleared
Malware Activity 80
Reconnaissance 8
Malicious Communication 29
Behavior Violation 6
Webservice Attack 0
Denial of Service 0
Application Violation 0
Security Weakness
69
0 Cleared
Blocked Port 69
Certificate Expiry 0
Weak Cipher 0
Open Port 0
AV Inactivity 0
IP Spoof 0
Mac Spoof 0
Latest Security Threats
4
0 Cleared
OpenSSL 3.0 Exploit Attempt 2
Log4j Prohibited Sites 1
OpenSSL 3.0 Vulnerability 1
URGENT/11 Attack 0
Bluekeep Attack 0
Ripple20 Attack 0
PrintNightmare Attack 0
Log4j Activity 0
Log4j Scan Activity 0



info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054