The Cadence Group Penetration Testing team performed a risk-based external security assessment against the computer network and supporting infrastructure of Ivanti Inc and the Ivanti Service Manager (ISM) application. This report is a summary of the complete penetration testing report dated December 2019.

Findings were a result of network and system discovery through automated and manual means. Findings also underwent additional validation steps to eliminate any potential false positives.

Methodology

Penetration testing is a methodical process comprised of reconnaissance, enumeration and scanning, and lastly, testing and validation.

The Cadence penetration test procedures are compiled from the following industry standard guidelines:

- NIST SP800-115, "Technical Guide to Information Security Testing and Assessment"
  - Available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- 2017 OWASP Top Ten Security Risks
  - Available at https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf
- Penetration Testing Execution Standard (PTES)
  - Available at http://www.pentest-standard.org)

Step 1: Reconnaissance

This phase included network enumeration through automated and manual means. This included the determination of alive network hosts and services available on those hosts. This effort was performed through network mapping, host discovery and network connection attempts, including:

- DNS enumeration
- Port scan / ping sweep of in-scope hosts
- Service detection / identification of answering, connectable services

Step 2: Vulnerability Identification

This phase attempted to identify publicly known vulnerabilities and evaluate their efficacy using automated and manual techniques, including:

- Vulnerability scanning of enumerated available services
- Web server configuration assessment
- Web application scanning (non-credentialed)
- Manual validation of automated findings

Step 3: Exploitation

The exploitation phase used the previous phases as input and targets an additional level of network access. Vulnerable services may respond unexpectedly to crafted network traffic, potentially allowing an escalation of privilege or service denial. This phase also produced proof-of-concept attack vectors, including:

- Additional network and information compromise targeted
- Full report with detailed exploitation techniques (where applicable)
- Custom scripting used for system or information compromise

Summary of Findings

The following graphic summarizes unresolved security issues by risk ranking:

External Network Assessment	High	Medium	Low
Findings	0	7	1

Risk Rating Definitions

High / Exploitable / Critical Vulnerabilities

The items in this category should receive priority consideration for risk analysis and remediation. These may be exploitable vulnerabilities, most likely with publicly accessible tools. They are trivially detected with industry standard scanners and pose the greatest level of risk to data confidentiality, integrity and/or availability.

Medium / Important Vulnerabilities

The vulnerabilities in this category should be treated as serious issues. They may not be immediately exploitable or the impact of exploit may be lower than those in the "High" category above, but represent known problems in software or configuration. They are easily detected by standard scanning techniques. Impact may be limited to accessibility (e.g. a host that is only accessible via local network access) or by what information could possibly be compromised (e.g. non-sensitive data). On their own, they may not represent a critical vulnerability, but if two or more are chained together, the impact may increase exponentially.

Low / Informational Vulnerabilities

Items listed in this category are noteworthy in the fact that they leak specific information that could be used in another attack vector or are related to an insecure protocol (e.g. FTP or telnet).