Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

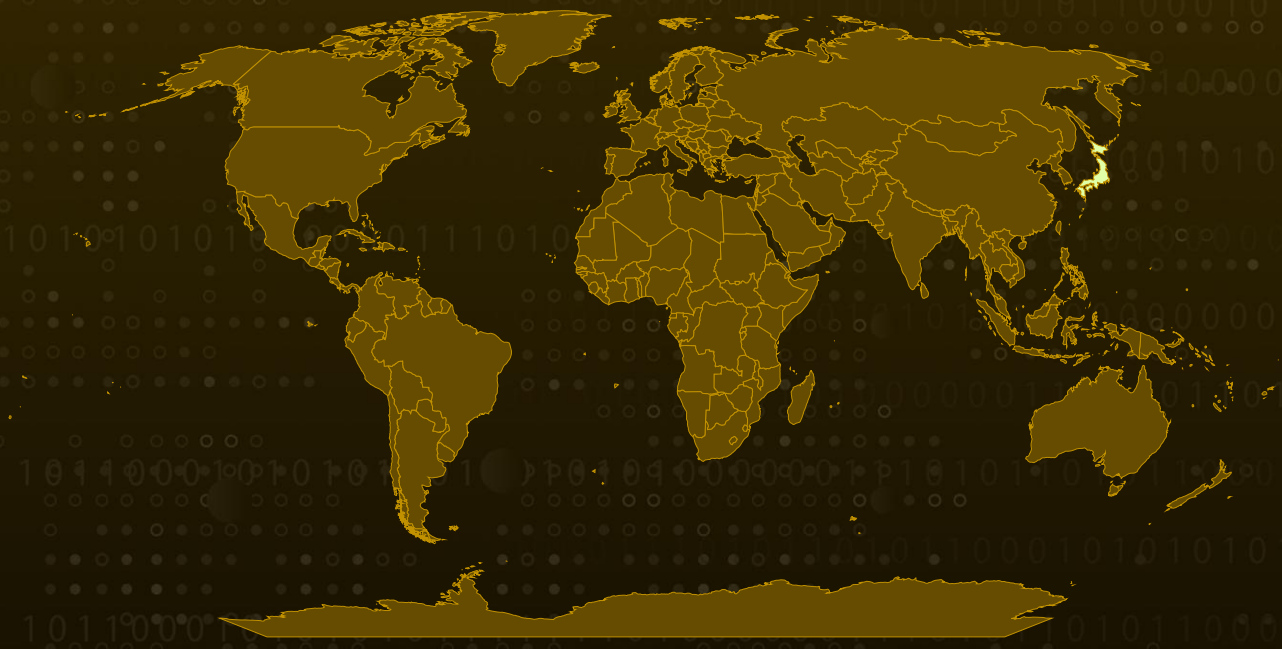
DslogdRAT Malware Exploits Ivanti Connect Secure Zero-Day Vulnerability

Date of Publication	Admiralty Code	TA Number
April 28, 2025	A1	TA2025130

Summary

Attack Discovered: December 2024
Targeted Countries: Japan
Malware: DslogdRAT
Affected Products: Ivanti Connect Secure, Policy Secure, and ZTA Gateways
Attack: A stealthy attack hit Japanese organizations in December 2024, exploiting a zero-day flaw (CVE-2025-0282) to silently deploy DslogdRAT malware. Using a hidden Perl-based web shell, the attackers gained control, with DslogdRAT quietly reaching out to its command server, executing commands, and blending into normal operations by only running during business hours.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	✓	✓

Attack Details

#1 In December 2024, organizations in Japan came under attack through a zero-day vulnerability tracked as CVE-2025-0282. The attackers planted a Perl-based web shell that quietly listened for incoming HTTP requests. When it detected a specific cookie value (af95380019083db5), it would execute any command the attackers sent, giving them full remote control. Through this hidden backdoor, they deployed a stealthy malware called DslogdRAT.

#2 DslogdRAT is built for persistence and stealth. Once running, it continuously cycles between periods of activity and sleep. It creates a second child process responsible for its main tasks: connecting to a command-and-control (C2) server, exchanging information, and carrying out instructions. The settings for these connections are hardcoded inside the malware, lightly obfuscated using a simple XOR method (0x63).

#3 To blend in with normal operations, DslogdRAT stays active only during typical office hours, between 8:00 AM and 8:00 PM, and remains dormant outside that window. While active, it can upload and download files, execute shell commands, and act as a proxy to support lateral movement across the network. Communications with its C2 server happen over socket connections, with basic encoding and decoding applied to the exchanged data.

#4 Alongside DslogdRAT, another malware family called SPAWNSNARE was also detected on the same compromised systems. The DslogdRAT malware illustrates how attackers' pair simple web shells with more sophisticated RATs to maintain persistence and control over compromised devices, highlighting the need for comprehensive security measures. Although the exact relationship between DslogdRAT and SPAWNSNARE remains unclear, their co-occurrence suggests a coordinated or multi-stage attack strategy targeting vulnerable Ivanti Connect Secure devices.

Recommendations

- **Update Immediately:** Fix known vulnerabilities like CVE-2025-0282 as soon as patches are available. Delaying updates gives attackers an easy way in.
- **Monitor Web Server Activity:** Keep an eye on unusual behavior, like unexpected uploads, strange cookie values, or hidden web shells. Set alerts for suspicious command executions.
- **Watch for Suspicious Network Traffic:** Track outgoing connections from servers. Malware like DslogdRAT tries to quietly talk to command servers catching strange traffic early can stop bigger problems.
- **Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0011** Command and Control	**T1608** Stage Capabilities
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1505** Server Software Component	**T1505.003** Web Shell
T1059 Command and Scripting Interpreter	**T1606** Forge Web Credentials	**T1606.001** Web Cookies	**T1140** Deobfuscate/Decode Files or Information

T1027 Obfuscated Files or Information	**T1205** Traffic Signaling	**T1082** System Information Discovery	**T1090** Proxy
T1571 Non-Standard Port	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1dd64c00f061425d484dd67b359ad99df533aa430632c55fa7e7617b55dab6a8, f48857263991eea1880de0f62b3d1d37101c2e7739dcd8629b24260d08850f9c, b1221000f43734436ec8022caaa34b133f4581ca3ae8eccd8d57ea62573f301d
File Path	/home/bin/dslogd, /home/webserver/htdocs/dana-na/cc/ccupdate.cgi, /bin/dsmain

Patch Link

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

References

https://blogs.jpcert.or.jp/en/2025/04/dslogdrat.html

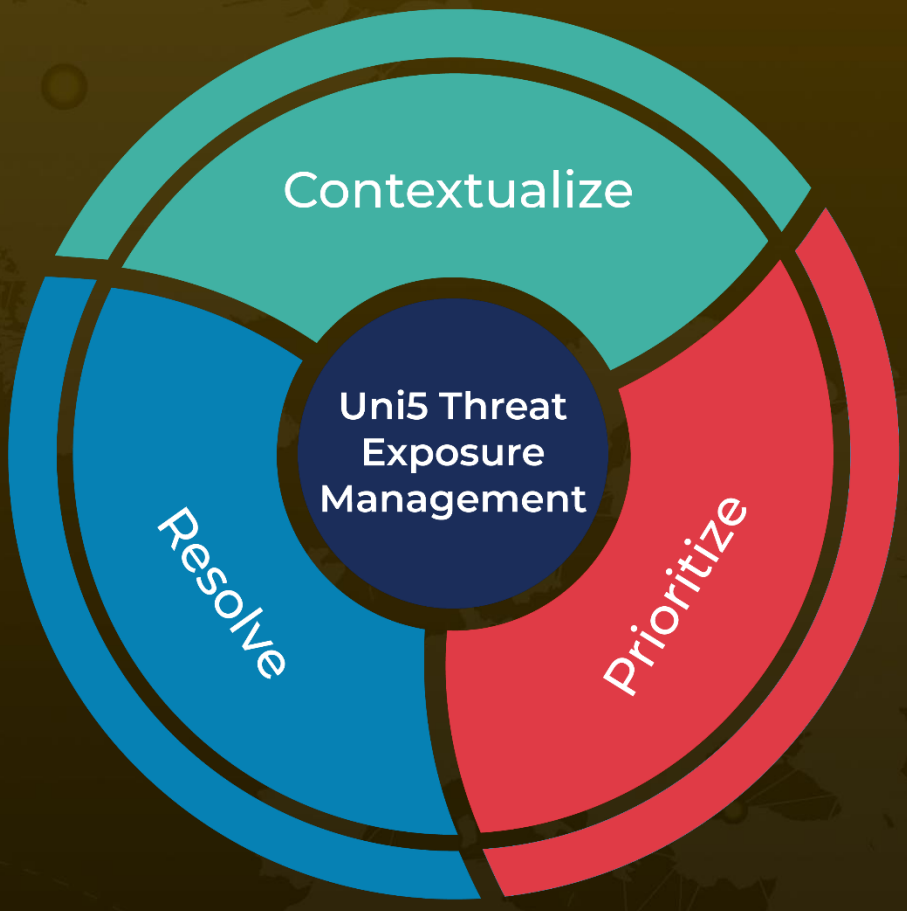
https://hivepro.com/threat-advisory/critical-ivanti-zero-day-flaw-exploited-in-the-wild/

https://hivepro.com/threat-advisory/cve-2025-22457-hackers-actively-exploiting-ivantis-critical-new-flaw/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 28, 2025 • 6:30 AM

More at www.hivepro.com